Preface

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

- Objective, page xv
- Audience, page xv
- Organization, page xvi
- Conventions, page xvii
- Related Documentation, page xviii
- Searching Cisco Documents, page xix
- Obtaining Documentation and Submitting a Service Request, page xix

Objective

This guide provides an overview and explains how to configure the various features for the Cisco 860, Cisco 880, and Cisco 890 series Integrated Services Routers (ISRs). 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 the *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.

Overview/Getting Started	
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.
Configuring the Router	
Configuring Power Managment	Describes the configuration of power management and Power-over-Ethernet (PoE).
Configuring Security Features	Provides procedures for implementing the security features that can be configured on the router.
Configuring Backup Data Lines and Remote Management	Provides procedures for configuring remote management functions and a backup data line connection.
Configuring Ethernet Switches	Provides an overview of the configuration tasks for the 4-port Fast Ethernet switch on the router.
Configuring Voice Functionality	Provides references to the procedures for voice configuration.
Configuring and Administering the Wireless Device	
Basic Wireless Device Configuration	Provides procedures for initial configuration of the wireless device.
Configuring Radio Settings	Describes how to configure radio settings for the wireless device.
Configuring WLAN	Describes configuration tasks for Cisco C866VAE-W-E-K9, C867VAE-W-A-K9, C867VAE-W-E-K9, and C867VAE-POE-W-A-K9 routers.
Administering the Wireless Device	Describes the various aspects of the administration of the wireless device.
Configuring Your Router for Ethernet and DSL Access	
Configuring PPP over Ethernet with NAT	Provides an overview of Point-to-Point Protocol over Ethernet (PPPoE) clients and network address translation (NAT)s that can be configured on the Cisco 860 and Cisco 880 series Integrated Services Routers (ISRs).
Configuring PPP over ATM with NAT	Provides an overview of Point-to-Point Protocol over Asynchronous Transfer Mode (PPPoA) clients and network address translation (NAT) that can be configured on the Cisco 860 and Cisco 880 series Integrated Services Routers (ISRs).

Configuring a LAN with DHCP and VLANs	Describes how the routers can use the Dynamic Host Configuration Protocol (DHCP) to enable automatic assignment of IP configurations for nodes on these networks.
Configuring a VPN Using Easy VPN and an IPSec Tunnel	Provides an overview of the creation of Virtual Private Networks (VPNs) that can be configured on the Cisco 860 and Cisco 880 series Integrated Services Routers (ISRs).
Additional Information	
Deployment Scenarios	Shows some typical deployment scenarios for the Cisco 860, Cisco 880, and Cisco 890 series ISRs.
Troubleshooting	Provides information to help isolate problems you might encounter.
Reference Information (Appendixes)	
Appendix A, "Cisco IOS Software Basic Skills"	Provides information for how to use Cisco IOS software to configure your router.
Appendix B, "Concepts"	Provides conceptual information that may be useful to Internet service providers or network administrators when they configure Cisco routers.
Appendix C, "ROM Monitor"	Provides information on how to use Cisco's ROM Monitor firmware.
Appendix D, "Common Port Assignments"	Lists currently assigned transmission control protocol (TCP) port numbers.

Conventions

These documents use the conventions listed in Table 1 to convey instructions and information.

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.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

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 the *Cisco 860, Cisco 880, and Cisco 890 Series ISR Software Configuration Guide* (this document), the Cisco 860, Cisco 880, and Cisco 890 series ISR documentation set includes the following documents:

- *Readme First for the Cisco 800 Series Integrated Services Routers.*
- *Cisco 860, Cisco 880, and Cisco 890 Series Integrated Services Routers Hardware Installation Guide*
- *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 12.4(15)XZ

You might 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 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, at:

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

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

CHAPTER 1

Product Overview

This chapter provides an overview of the features available for the Cisco 860, Cisco 880, and Cisco 890 series Integrated Services Routers (ISRs), and contains the following sections:

- General Description, page 1-1
- Cisco 860 Series ISRs, page 1-1
- Cisco 880 Series ISRs, page 1-4
- Cisco 890 Series ISRs, page 1-8
- Licensing, page 1-9

General Description

The Cisco 860, Cisco 880, and Cisco 890 series ISRs provide Internet, VPN, voice, 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 860W, Cisco 880W, and Cisco 890W series ISRs incorporate an 802.11n wireless LAN option that allows the ISR to act as a wireless access point.

Cisco 860 Series ISRs

This section contains the following topics:

- Cisco 860 Series ISR Features, page 1-1
- Cisco 860VAE Series ISR Features, page 1-2

Cisco 860 Series ISR Features

The Cisco 860 series ISRs are fixed-configuration data routers that provide either a 10/100 Fast Ethernet (FE) or an ADSL2 over POTs WAN connection.

The following features are supported on all Cisco 860 series ISRs:

- 4-port 10/100 FE LAN Switch, page 1-2
- Security Features, page 1-2
- 802.11n Wireless LAN Option, page 1-2

4-port 10/100 FE LAN Switch

This switch provides four ports for connecting to 10/100BASE-T (10/100 Mbps) Fast Ethernet (FE) LANs or access points.

Security Features

The Cisco 860 platforms provide the following security features:

- IPsec
- Firewall

802.11n Wireless LAN Option

The Cisco 861W ISR has an integrated 802.11b/g/n single radio module for wireless LAN connectivity. With this module, the router can then act as an access point in the local infrastructure.

Cisco 860VAE Series ISR Features

The following sections describe the features of the Cisco 860VAE series ISRs:

- General Features, page 1-2
- Interfaces, page 1-3
- IOS Images, page 1-4

General Features

Table 1-1 describes the general features of Cisco 860VAE series routers.

Table 1-1 General Features of Cisco 860VAE Series ISRs

Feature	Benefit
Increased performance	• Performance enables customers to take advantage of broadband network speeds while running secure, concurrent data, voice, video, and wireless services.
Security and QoS with secure routers	• IPSec & Easy VPN with 10 tunnels. • BGP. • MAC filtering and port security. • QoS features include LLQ and WFQ. • NBAR and DiffServ.
State-of-the-art xDSL	• State-of-the-art xDSL features, including latest ADSL2+/VDSL2 standards. • Improved interoperability vs. various DSLAMs deployed at WW SPs.

Table 1-1 General Features of Cisco 860VAE Series ISRs

Feature	Benefit
ScanSafe web filtering	• Protects network and staff from undesirable web content • Increases productivity by limiting time spent on recreational surfing • Optimizes network resources by reducing bandwidth congestion • Monitors online activity with comprehensive reporting
IPv6 support	• Supports latest IP addressing standards
WAN Diversity	• GE + DSL multimode VDSL2 and ADSL 1, 2, and 2+. • Multiple WAN options within the same box allow consistent configuration across diverse deployments.
Four-port 10/100-Mbps managed switch 1 GE port for secure routers	• Connection of multiple devices within a teleworker home or a small office, with the ability to designate a port as the network edge. • VLANs allow for secure segmentation of network resources.
CON/AUX port	• A single dual-purpose port provides direct connection to a console or external modem for management or backup access points.
Real-time clock	• A built-in real-time clock maintains an accurate date and time for applications that require an accurate time stamp, such as logging and digital certificates.

Interfaces

Table 1-2 describes the interfaces of the Cisco 860VAE series routers.

Table 1-2 Interfaces of the Cisco 860VAE Series ISRs

	Model			
Interfaces	866VAE	867VAE	866VAE-K9	867VAE-K9
4 FE[1] switch ports	x	x	x	x
1 GE[2] switch port	—	—	x	x
1 GE WAN port	x	x	x	x
1 VDSL/ADSL over POTS port	—	x	—	x
1 VDSL/ADSL over ISDN port	x	—	x	—

[1] FE = Fast Ethernet

[2] GE = Gigabit Ethernet

Note The Cisco 866VAE, 867VAE, 866VAE-K9, and 867VAE-K9 routers each have two WAN ports. Only one of the two ports can be active at any given time.

IOS Images

Table 1-3 describes the IOS images included in Cisco 860VAE series routers.

Table 1-3 IOS Images of the Cisco 860VAE Series ISRs

	Model			
IOS Image	**866VAE**	**867VAE**	**866VAE-K9**	**867VAE-K9**
c860vae-ipbasek9-mz	x	x	—	—
c860vae-advsecurityk9-mz	—	—	x	x
c860vae-advsecurityk9_npe-mz	—	—	x	x

Cisco 880 Series ISRs

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

- Models of the Cisco 880 Series ISRs, page 1-4
- Common Features, page 1-7
- Voice Features, page 1-7

Models of the Cisco 880 Series ISRs

The Cisco 880 series ISRs have data and voice capabilities. Each router has one WAN port. In addition, routers supporting voice have either FXS (Foreign Exchange Station) or BRI voice ports. Data or voice backup ports are also available on most of the routers. The Cisco 880G routers come with a commercial third-generation (3G) wireless interface card that provides cellular backup. 802.11b/g/n option is available on all models.

Table 1-4 gives the port configurations of the Cisco 880 series data routers.

Table 1-4 Port Configurations of the Cisco 880 Series Data ISRs

		Backup	
Model	**WAN Port**	**Data ISDN**	**Data 3G**
881 and 881W	FE	—	—
881-V	FE	—	—
881G and 881GW	FE	—	x
886 and 886W	ADSL2oPOTS	x	—
886G and 886GW	ADSL2oPOTS	—	x
887 and 887W	ADSL2oPOTS	x	—
887G and 887GW	ADSL2oPOTS	—	x
887-VA-V	VDSL2oPOTS	x	x
887V and 887VW	VDSL2oPOTS	x	—

Table 1-4 Port Configurations of the Cisco 880 Series Data ISRs (continued)

		Backup	
Model	WAN Port	Data ISDN	Data 3G
887VG and 887VGW	VDSL2oPOTS	—	x
888 and 888W	G.SHDSL	x	—
888G and 888GW	G.SHDSL	—	x
888E and 888EW	EFM over G.SHDSL	x	—
C888EA-K9	Multimode	x	—

Table 1-5 gives the port configurations of the Cisco 880 series voice routers.

Table 1-5 Port Configurations of the Cisco 880 Series Voice ISRs

			Backup	
Model	WAN Port	FXS Voice Ports	PSTN FXO	PSTN BRI
C881SRST and C881SRSTW	FE	4	x	—
C888SRST and C888SRSTW	G.SHDSL	4	—	x
C888ESRST and C888ERSTW	EFM over G.SHDSL	4	—	4

Table 1-6 gives the port configurations of the Cisco 881-V, Cisco887VA-V and Cisco 887VA-V-W routers.

Table 1-6 Port Configurations of the Cisco 880 Series Data and Voice ISRs

					Backup	
Model	WAN Port	FXS Voice Ports	PSTN BRI	WLAN	PSTN FXO	Data (ISDN)
C881-V	FE	4	2	—	1	—
C887VA-V	VDSL2/ADSL2	4	2	—	—	x
C887VA-V-W	VDSL2/ADSL2	4	2	x	—	x

The Cisco 887 VA-V and Cisco 881-V routers give you the flexibility to use the FXS or BRI voice ports (The Cisco 881-V router also supports a backup FX0 port), but the number of concurrent calls that the router supports is limited by the codec complexity configuration. The router supports less calls when the codec complexity setting is configured for high complexity. Table 1-7 shows the number of concurrent calls that is supported on the router for each codec complexity setting. Configuring the codec complexity setting to support secure calls does not affect the numbers below.

Table 1-7 Number of Concurrent Calls Supported

	Flexible Complexity	Medium Complexity	High Complexity
C881-V	9	8	6
C887VA-V	8	8	6
C887VA-V-W	8	8	6

Common Features

Cisco 880 series ISRs support the following features:

- 4-port 10/100 FE LAN Switch, page 1-7
- 802.11n Wireless LAN Option, page 1-7
- Real-Time Clock, page 1-7
- Security Features, page 1-7

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. In addition, an upgrade is available that gives Power over Ethernet (PoE) on two of the ports to provide power to access points or phones.

802.11n Wireless LAN Option

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

Real-Time Clock

A real-time clock (RTC) provides 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.

Security Features

The Cisco 880 platforms provide the following security features:

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

Voice Features

The Cisco 880 voice and data platforms (C880SRST, C880SRSTW, C881-V, C887 VA-V, and C887VA-V-W) support the following voice features:

- Signaling protocols: Session Initiation Protocol (SIP), Media Gateway Control Protocol (MGCP), and H323
- Real-time transfer protocol (RTP), Cisco RTP (cRTP), and secure RTP (SRTP) for these signaling protocols
- Fax passthrough, Cisco fax relay, T37 fax store-and-forward, and T.38 fax relay (including T.38 gateway-controlled MGCP fax relay)

- Dual tone multifrequency (DTMF) Relay—OOB and RFC2833
- Silence suppression/comfort noise
- G.711 (a-law and u-law), G.729A, G.729AB, G.729, G.729B, G.726
- Support of SRST failover to a Foreign Exchange Office (FXO) or BRI backup port connected to PSTN in case of WAN failure on C880SRST and C880SRSTW.
- Support for SRST and CME requires user license, but only a 5-user license is supported on C881-V, C887VA-V, and C887VA-V-W routers.
- Direct inward dialing (DID) on FXS

Cisco 890 Series ISRs

The Cisco 890 series ISRs are fixed-configuration data routers. These routers have a Gigabit Ethernet WAN port and data backup ports.

Table 1-8 gives the port configurations for the Cisco 890 Series ISRs.

Table 1-8 Port Configurations of the Cisco 890 Series ISRs

		Data Backup		
Model	**WAN Port**	**FE**	**V.92**	**ISDN**
891 and 891W	GE	x	x	—
892 and 892W	GE	x	—	x
892F and 892F-W	GE[1] or SFP[2]	x	—	x

[1] GE copper port.

[2] SFP port supports GE with fiber. For a complete list of SFPs supported, see the Cisco 892F ISR data sheet on Cisco.com.

The following features are supported:

- 8-port 10/100 FE LAN Switch, page 1-8
- 802.11n Wireless LAN Option, page 1-8
- Real-Time Clock, page 1-9
- Security Features, page 1-9

8-port 10/100 FE LAN Switch

This switch provides eight ports for connecting to 10/100BASE-T FE LANs, access points, or IP phones. In addition, an upgrade is available that gives PoE on four of the ports to provide power to access points or phones.

802.11n Wireless LAN Option

The Cisco 890W series ISRs have integrated 802.11b/g/n and 802.11a/n dual radio modules for wireless LAN connectivity. With these modules, the router can act as an access point in the local infrastructure.

Real-Time Clock

A real-time clock (RTC) provides 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.

Security Features

The Cisco 890 platforms provide the following security features:

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

Licensing

The Cisco 860, Cisco 880, and Cisco 890 ISRs ship with licensed software installed. Software features may be upgraded and the software licenses may be managed through *Cisco Licensing Manager*. See *Software Activation On Cisco Integrated Services Routers and Cisco Integrated Service Routers G2* for details.

When you order a new router, you specify the software image and feature set that you want. 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.

Note The Cisco 860VAE does not require licenses.

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 860, Cisco 880, and Cisco 890 platforms, see *Cisco 860 Data Sheet*, *Cisco 880 Data Sheet*, and *Cisco 890 Data Sheet*. See *Cisco IOS Software Activation Tasks and Commands* for details about how to activate and manage the software licenses.

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 of an access point 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™, 802.11a-compliant, 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 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 Leightweight 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.

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

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

Note Avoid using the CLI and the web-browser tools concurrently. If you configure the wireless device using the CLI, the web-browser interface may display an inaccurate interpretation of the configuration.

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

Network Configuration Examples

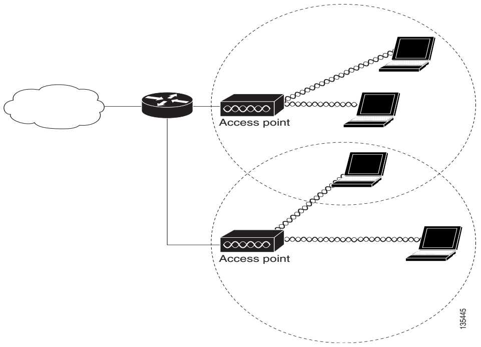
Set up the access point role in any of these common wireless network configurations. The access point default configuration is as a root unit connected to a wired LAN or as the central unit in an all-wireless network. Access points can also be configured as bridges and workgroup bridges. These roles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

- Root Access Point, page 2
- Central Unit in an All-Wireless Network, page 3

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.

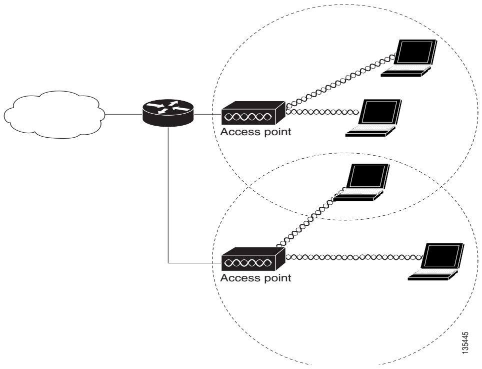
Figure 2-1 Access Points as Root Units on a Wired LAN



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, and contains the following sections:

- Interface Ports, page 3-2
- Default Configuration, page 3-3
- Information Needed for Configuration, page 3-4
- Configuring Command-Line Access, page 3-5
- Configuring Global Parameters, page 3-7
- Configuring WAN Interfaces, page 3-8
- Configuring the Fast Ethernet LAN Interfaces, page 3-55
- Configuring the Wireless LAN Interface, page 3-55
- Configuring a Loopback Interface, page 3-55
- Configuring Static Routes, page 3-57
- Configuring Dynamic Routes, page 3-58

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.

For complete information on how to access global configuration mode see Entering Global Configuration Mode, page A-5.

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
LAN Ports		
Cisco 860, Cisco 880, and Cisco 890 series	Fast Ethernet LAN	LAN, FE0–FE3
	Wireless LAN	(no label)
Cisco 866VAE, 867VAE	Ethernet LAN	LAN, FE0-FE3
Cisco 866VAE-K9, 867VAE-K9	Ethernet LAN	LAN, GE0, FE0-FE3
WAN Ports		
Cisco 861, 861W, 881, 881W, 881G, 881GW, 881-V	Fast Ethernet WAN	WAN, FE4
Cisco 867, 867W	ADSL2oPOTS WAN	ADSLoPOTS
Cisco 886, 886W, 886G, 886GW	ADSL2oISDN WAN	ADSLoPOTS
Cisco 887, 887W	ADSL2oPOTS WAN	ADSLoPOTS
Cisco 887V, Cisco887VW, 887VG, 887VGW	VDSL2oPOTS WAN	VDSLoPOTS
Cisco 867VA, 887VA, 887VA-M, 887VA-V, 887VA-V-W	VDSL/ADSLoPOTS WAN	VDSL/ADSLoPOTS
Cisco 888, 888W	G.SHDSL WAN	G.SHDSL
Cisco 891, 892	Fast Ethernet WAN	FE8
	Gigabit Ethernet WAN	WAN GE 0
Cisco 866VAE, 867VAE	Gigabit Ethernet WAN	WAN GE0
Cisco 866VAE-K9, 867VAE-K9	Gigabit Ethernet WAN	WAN GE1
Cisco 866VAE, 866VAE-K9	VDSL/ADSLoISDN WAN	VDSL/ADSL OVER ISDN
Cisco 867VAE, 867VAE-K9	VDSL/ADSLoPOTS WAN	VDSL/ADSL OVER POTS

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

Gather 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 collecting the appropriate information, perform a full configuration on your router beginning with the tasks in "Configuring Command-Line Access" section on page 3-5.

If you plan to:

- Connect voice equipment, see *Cisco IOS Voice Port Configuration Guide*.
- 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, perform the following 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`	Enables password checking at terminal session login.
Step 4	**exec-timeout** *minutes* [*seconds*] **Example:** `Router(config-line)# exec-timeout 5 30`	Sets the time 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`	Specifies a virtual terminal for remote console access.
Step 6	**password** *password* **Example:** `Router(config-line)# password aldf2ad1`	Specifies a unique password for the virtual terminal line.

	Command	Purpose
Step 7	**login** **Example:** `Router(config-line)# login`	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, perform 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# configure terminal`
		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`	Specifies the name for the router.
Step 3	**enable secret** *password* **Example:** `Router(config)# enable secret cr1ny5ho`	Specifies an encrypted password to prevent unauthorized access to the router.
Step 4	**no ip domain-lookup** **Example:** `Router(config)# no ip domain-lookup`	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 3-9
- Configuring the Media Type, page 3-10
- Configuring a Gigabit Ethernet WAN Interface, page 3-10
- Configuring a V.92 Modem Interface, page 3-11
- Configuring a VDSL2 WAN Interface, page 3-12
- Configuring ADSL or VDSL on Cisco 860VAE and 880VA Multimode ISRs, page 3-14
- Configuring Seamless Rate Adaption, page 3-16
- Configuring UBR+, page 3-16
- Configuring ADSL Mode, page 3-17
- Configuring VDSL Mode, page 3-24
- Configuring the Training Log Using the CLI, page 3-34
- Configuring a G.SHDSL WAN Interface in ATM mode, page 3-36
- Configuring a G.SHDSL WAN Interface in EFM mode, page 3-40
- Configuring the Cellular Wireless WAN Interface, page 3-40
- Configuring WAN Mode on Cisco 860VAE ISRs, page 3-52

Configuring a Fast Ethernet WAN Interface

To configure the Fast Ethernet interface on a Cisco 861 or 881 ISR, perform 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`	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`	Sets the IP address and subnet mask for the specified Fast Ethernet interface.
Step 3	**no shutdown** **Example:** `Router(config-if)# no shutdown`	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.

Note Cisco IOS Release 15.1 (3) T introduces the **batch** command under the interface mode. You may notice a reduced CPU utilization when interface batching is enabled because packets are processed in batches resulting in more efficient cache usage.

Configuring the Media Type

Before configuring the Gigabit Ethernet interface on the Cisco 892F ISRs, you must first select the media type as either SFP or RJ45.

To configure the media type, perform the following steps, begining in global configuration mode:

SUMMARY STEPS

1. **interface** *type number*
2. **media-type** {**sfp** | **rj45**}
3. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0`	Enters the configuration mode for a Gigabit Ethernet WAN interface on the router.

Step 2	**media-type** {**sfp** | **rj45**}
	Example:
	`Router(config-if)# media-type sfp`
	`OR`
	`Router(config-if)# media-type rj45`
		Specifies an SFP physical connection.
		OR
		Specifies an RJ-45 physical connection.

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

Configuring a Gigabit Ethernet WAN Interface

To configure the Gigabit Ethernet (GE) WAN interface on a Cisco 891, 892, or 860VAE ISR, perform 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 gigabitethernet 1`
	`Router(config-if)#`
		Enters the configuration mode for a Gigabit 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`	Sets the IP address and subnet mask for the specified Gigabit Ethernet interface.
Step 3	**no shutdown** **Example:** `Router(config-if)# no shutdown`	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 Gigabit Ethernet interface and returns to global configuration mode.

Configuring a V.92 Modem Interface

The Cisco 891 ISR has a V.92 modem backup interface. To configure this interface, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **interface** *type number*
2. **ip address** *ip-address mask*
3. **encapsulation** *ppp*
4. **dialer in-band**
5. **dialer string** *dial-string*
6. **dialer-group** *group-number*
7. **async mode dedicated**
8. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	**interface** *type number* **Example:** `Router(config)# interface async 1`	Enters the configuration mode for a V.92 WAN interface (serial 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`	Sets the IP address and subnet mask for the specified V.92 interface.
Step 3	**encapsulation** *ppp* **Example:** `Router(config-if)# encapsulation ppp`	Sets the encapsulation method to point-to-point protocol (PPP) for the serial interface.
Step 4	**dialer in-band** **Example:** `Router(config-if)# dialer in-band`	Specifies that dial-on-demand routing (DDR) is supported.
Step 5	**dialer string** *dial-string* **Example:** `Router(config-if)# dialer string 102`	Specifies the string (telephone number) to be used when placing a call from the interface.
Step 6	**dialer-group** *group-number* **Example:** `Router(config-if)# dialer-group 1`	Configures the interface to belong to a specific dialing access group.
Step 7	**async mode dedicated** **Example:** `Router(config-if)# async mode dedicated`	Places the line into dedicated asynchronous mode using Serial Line Internet Protocol (SLIP) or PPP encapsulation.

Step 8	**exit**
	Example:
	`Router(config-if)# exit`
	`Router(config)#`
		Exits configuration mode for the V.92 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 that the VDSL2 WAN interface uses Ethernet as the Layer 2 transport mechanism.

To configure VDSL2 on the Cisco 887V ISR, perform 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)# controller vdsl 0`	Enters controller configuration mode and the controller number. **Note** There is no need to configure any VDSL2 parameters from CPE side. Any specific VDSL2 settings should be set on the DSLAM side.
Step 2	**interface** *type number* **Example:** `Router(config)# interface ethernet 0`	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`	Sets the IP address and subnet mask for the interface.
Step 4	**shutdown** **Example:** `Router(config-if)# no shutdown`	Disables the interface, changing its state from administratively up to administratively down.
Step 5	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the interface, changing its state from administratively down to administratively up.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits configuration mode and returns to global configuration mode.

Configuring ADSL or VDSL on Cisco 860VAE and 880VA Multimode ISRs

This section covers the following topics:

- Overview of Cisco 860VAE, 886VA, and 887VA Multimode ISRs, page 3-14
- ADSL2/2+ Annex M Mode on Over POTS VDSL2/ADSL Multimode Annex A SKUs, page 3-15
- Enabling ADSL2/2+ Annex M Mode on Over POTS VDSL2/ADSL Multimode Annex A SKUs, page 3-30

Overview of Cisco 860VAE, 886VA, and 887VA Multimode ISRs

The Cisco customer premise equipment (CPE) Cisco 866VAE, 867VAE, 866VAE-K9, 867VAE-K9, 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 multimode.

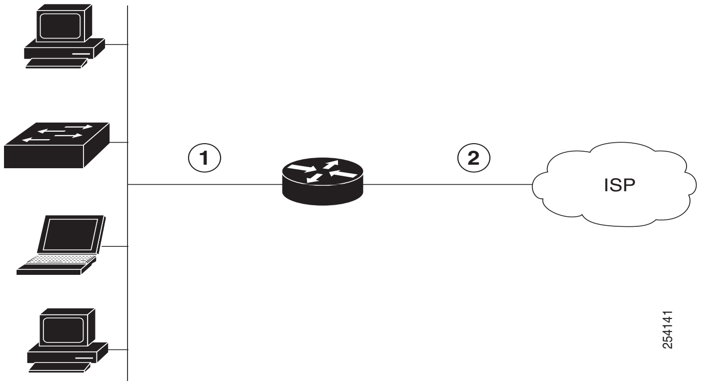
Note The 866VAE and 886VA support xDSL over ISDN. The 867VAE and 887VA support xDSL over a plain old telephone system (POTS).

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 mode, 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 or Gigabit Ethernet LAN interface	**2**	ATM WAN interface—ADSL 1/2/2+ 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).

Note Cisco 866VAE, Cisco 867VAE, Cisco 866VAE-K9, and Cisco 867VAE-K9 ISRs allow a maximum of two PVCs.

ADSL2/2+ Annex M Mode on Over POTS VDSL2/ADSL Multimode Annex A SKUs

Annex M is an enhancement of the G.992.3 standard that doubles the upstream bandwidth by "borrowing" 32 additional tones from the downstream frequency range. This feature enables service providers to provision symmetric data rates for ADSL2 and ADSL2+ services with data rates up to 2 Mbps.

Cisco IOS Release 15.2(1)T adds support for enabling Annex M data structures on Cisco 887VA platforms and Annex A data structures on Cisco 887VA-M platforms. This features allows both Annex A and Annex M structures to be run on the same platform with a performance tradeoff for the annex that is not optimized for the device. With this feature implementation, the modes supported on Annex A platforms are the same as the modes supported on Annex M platforms (887VA-M and EHWIC-1DSL-VA-M). When digital subscriber line access multiplexer (DSLAM) supports Annex M, Annex M mode takes precedence over Annex A mode.

Note Cisco 867VAE and 867VAE-K9 require Cisco IOS Release 15.1(4)M2 or 15.2(2)T or later to use this feature.

For information on configuring Annex M data structures on Annex A platforms, see the, "Enabling ADSL2/2+ Annex M Mode on Over POTS VDSL2/ADSL Multimode Annex A SKUs" section on page 3-30.

Configuring Seamless Rate Adaption

ADSL connections can be dropped due to a number of reasons, such as crosstalk, changes in noise margin, temperature changes, or interference. ADSL2 addresses these problems by adapting the data rate in real-time. Seamless rate adaptation (SRA) enables the ADSL2 system to change the data rate of the connection during operation without any service interruption or bit errors.

Note These features are not currently available on the 866VAE, 867VAE, 866VAE-K9, and 867VAE-K9.

For information on configuring SRA, see the "Enabling Seamless Rate Adaption" section on page 3-31.

Configuring UBR+

UBR is typically used for data communications applications, such as file transfer and email. UBR is a best effort service and is the lowest class of service in the hierarchy. There are no guarantees to the actual bandwidth allowed. Therefore, UBR virtual circuits (VCs) are susceptible to a large number of cell drops or a high cell transfer delay as cells move from the source to the destination. UBR has no bounds on Cell Delay Variation Tolerance (CDVT) and is only a best effort service.

UBR+ is a special ATM service class developed by Cisco. UBR defines only peak cell rate (PCR); however, UBR+ defines a minimum guaranteed cell rate (MCR) and (on the switch) a cell delay variation tolerance (CDVT).

Note On Cisco IOS versions 15.2(1)T and later, UBR+ is compatable with Cisco Multimode 886VA and 887VA routers.

Note These features are not currently available on the 866VAE, 867VAE, 866VAE-K9, and 867VAE-K9.

For information on configuring UBR+, see the "Configuring UBR+" section on page 3-32.

Configuring ADSL Mode

Configuration tasks

Perform the following tasks to configure ADSL mode:

- Configuring ADSL Auto Mode, page 3-17
- Configuring CPE and Peer for ADSL Mode, page 3-18
- Verifying ADSL Configuration, page 3-22
- Verifying CPE to Peer Connection for ADSL, page 3-24

Configuring ADSL Auto Mode

Perform these steps to configure the DSL controller to auto mode, starting in global configuration mode.

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller vdsl** *slot*
4. **operating mode {auto | adsl1 | adsl2 | adsl2+ | vdsl2 | {ansi |etsi}}**

   Note The ansi option is available only for models that support POTS. The etsi option is available only for models that support ISDN.

5. **end**

DETAILED STEPS

	Command	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**controller vdsl** *slot* **Example:** `Router(config)# controller vdsl 0`	Enters config mode for the VDSL controller.

	Command	Purpose

Step 4	**operating mode {auto | adsl1 | adsl2 | adsl2+ | vdsl2 | ansi}**
	Example:
	`Router(config-controller)# operating mode auto`
		Configures the operating mode. The default is auto and is recommended.
		Note When configured in auto, the operating mode does not appear in the **show running** command.

Step 5	**end**
	Example:
	`Router(config-controller)# end`
	`Router#`
		Exits the configuration mode and enters EXEC mode.
		Note A reload is required after changing mode between adsl and vdsl for Cisco 866VAE, Cisco 867VAE, Cisco 866VAE-K9, and Cisco 867VAE-K9.

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.

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

Configuring the ATM CPE side

Perform the following steps to configure the ATM CPE side, starting in global configuration mode.

	Command	Purpose

Step 1	**interface** *type number*
	Example:
	`Router(config)# interface atm0`
	`Router(config-if)#`
		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.

	Command	Purpose

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

Configuring the ATM Peer side

Perform the following steps to configure the ATM peer side, starting in global configuration mode.

	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`	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`	Enables the ATM0.1 point-to-point interface.

	Command	Purpose
Step 4	**ip address** *ip-address mask* **Example:** `Router(config-subif)# ip address 30.0.0.2 255.255.255.0`	Enters IP address and subnet mask.
Step 5	**pvc [name] vpi/vci** **Example:** `Router(config-subif)# pvc 13/32`	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 30.0.0.1 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 advipservices
!
!
vtp domain cisco
vtp mode transparent
!
!
controller VDSL 0
!
vlan 2-4
!
!
!
!
!
interface Ethernet0
 no ip address
 shutdown
 no fair-queue
!
interface BRI0
 no ip address
 encapsulation hdlc
 shutdown
 isdn termination 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-plane
!
!
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 from 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:         'BDCM'                   '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 Near:    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
Attainable 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          File Name (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 set up 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 VDSL Mode

Configuration tasks

Perform the following tasks to configure VDSL mode:

- Configuring VDSL Auto Mode, page 3-24
- Configuring CPE and Peer for VDSL Mode, page 3-25
- Verifying VDSL Configuration, page 3-28
- Verifying CPE to Peer Connection for VDSL, page 3-30

Configuring VDSL Auto Mode

Perform the following steps to configure the DSL controller to auto mode, starting in global configuration mode.

Note Configure the DSLAM in VDSL2 mode prior to configuring the router.

SUMMARY STEPS

1. **controller vdsl** *slot*
2. **operating mode {auto | adsl1 | adsl2 | adsl2+ | vdsl2 | {ansi |etsi}}**

   Note The ansi option is available only for models that support POTS. The etsi option is available only for models that support ISDN.

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 | ansi}**
	Example:
	`Router(config-controller)# operating mode auto`
		Configures the operating mode. The default is auto and is recommended.
		Note When configured in auto, the operating mode does not appear in the **show running** command.

Step 3	**end**
	Example:
	`Router(config-controller)# end`
	`Router#`
		Exits the configuration mode and enters EXEC mode.
		Note A reload is required after changing the mode on the Cisco 866VAE, Cisco 867VAE, Cisco 866VAE-K9, and Cisco 867VAE-K9.

Configuring CPE and Peer for VDSL Mode

When configuring VDSL, configure the ethernet 0 interface and perform a **no shutdown** command on the interface if needed. Start in the global configuration mode.

Configuring the VDSL CPE Side

Perform the following steps to configure the VDSL CPE side, starting in the global configuration mode.

SUMMARY STEPS

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

DETAILED STEPS

	Command	Purpose
Step 1	**interface** *type number* **Example:** `Router(config)# interface ethernet0`	Enters configuration mode for the Ethernet interface 0.
Step 2	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 90.0.0.1 255.255.255.0`	Enters the IP address and subnet mask.
Step 3	**no shutdown** **Example** `Router(config-if)# no shutdown`	Enables the configuration changes to the ip address and subnet mask.

Step 4	**end**
	Example
	`Router(config-if)# end`
	`Router#`
		Exits the configuration mode and enters EXEC mode.

Configuring the VDSL Peer Side

Perform the following steps to configure the VDSL Peer side, starting in the global configuration mode.

	Command	Purpose
Step 1	**interface** *type number* **Example:** `Router(config)# interface ethernet0`	Enters configuration mode for the Ethernet interface 0.
Step 2	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 90.0.0.2 255.255.255.0`	Configures the IP address and subnet mask.
Step 3	**no shutdown** **Example** `Router(config-if)# no shutdown`	Enables the configuration changes to the IP address and subnet mask.

Step 4	**end**
	Example
	`Router(config-if)# end`
	`Router#`
		Exits the configuration mode and enters EXEC mode.

VDSL Configuration Example

The following example shows a typical output of a VDSL configuration. 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 advipservices
!
!
vtp domain cisco
vtp mode transparent
!
!
controller VDSL 0
!
vlan 2-4
!
!
!
!
!
interface Ethernet0
 ip address 30.0.0.1 255.255.255.0
 no fair-queue
!
interface BRI
 no ip address
 encapsulation hdlc
 shutdown
 isdn termination multidrop
!
```

```
interface ATM0
 no ip address
 shutdown
!
!
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-plane
!
!
line con 0
 no modem enable
line aux 0
line vty 0 4
 login
 transport input all
!
exception data-corruption buffer truncate
end
```

Verifying VDSL Configuration

Verify the configuration is set properly by using the **show controller vdsl 0** command from 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:         'BDCM'                   'BDCM'
Chip Vendor Specific:   0x0000                   0x0000
Chip Vendor Country:    0xB500                   0xB500
Modem Vendor ID:        'CSCO'                   'BDCM'
Modem Vendor Specific:  0x4602                   0x0000
Modem Vendor Country:   0xB500                   0xB500
Serial Number Near:    FHK1313227E 887-V2-K 15.1(20100
Serial Number Far:
Modem Version Near:    15.1(20100426:193435) [changahn
Modem Version Far:     0x0000


Modem Status:            TC Sync (Showtime!)
DSL Config Mode:         AUTO
Trained Mode:            G.993.2 (VDSL2) Profile 12a
TC Mode:                 PTM
Selftest Result:         0x00
DELT configuration:      disabled
DELT state:              not running
Trellis:                 ON                       OFF
Line Attenuation:         1.0 dB                  0.0 dB
Signal Attenuation:       1.0 dB                  0.0 dB
Noise Margin:            12.0 dB                  9.5 dB
Attainable Rate:        87908 kbits/s            50891 kbits/s
Actual Power:           13.5 dBm                  8.9 dBm
Per Band Status:        D1      D2      D3      U0      U1      U2      U3
Line Attenuation(dB):   0.9     2.3     N/A     7.2     2.9     7.0     N/A
Signal Attenuation(dB): 0.9     2.3     N/A     N/A     2.3     6.6     N/A
Noise Margin(dB):       14.5    9.3     N/A     N/A     N/A     N/A     N/A
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:               1                        0


Full inits:             33
Failed full inits:      0
Short inits:            0
Failed short inits:     0


Firmware        Source          File Name (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            84999             0             48968
Previous Speed:           0            24184             0              1047
Reed-Solomon EC:          0                0             0                 0
CRC Errors:               0                0             0                 0
Header Errors:            0                0             0                 0
Interleave (ms):       0.00             6.00          0.00              0.00
Actual INP:            0.00             0.00          0.00              0.00


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


Router#
```

Verifying CPE to Peer Connection for VDSL

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#
```

Enabling ADSL2/2+ Annex M Mode on Over POTS VDSL2/ADSL Multimode Annex A SKUs

To enable ADSL2/2+ Annex M mode on Over POTS VDSL2/ADSL Multimode Annex A SKUs, perform the following steps.

Note This feature requires Cisco IOS Release 15.2(1)T or a later.

Note Cisco 867VAE and 867VAE-K9 require Cisco IOS Release 15.1(4)M2 or 15.2(2)T or later to use this feature.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller vdsl** *0*
4. **operating mode {adsl1 | adsl2 [***annex a* | *annex m***] | adsl2+ [***annex a* | *annex m***]| ansi | auto| vdsl2 }**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**`controller vdsl`** *`0`*	Enters configuration mode for the VDSL controller.

Step 4	**operating mode** {**adsl1** | **adsl2** [*annex a* | *annex m*] | **adsl2+** [*annex a* | *annex m*] | **ansi** | **auto**| **vdsl2**}
	Example:
	`Router(config-controller)# operating mode adsl2+ annex m`
		asdl1—Configures operation in ITU G.992.1 Annex A full-rate mode.
		adsl2—Configures operation in ADSL2 operating mode-ITU G.992.3 Annex A, Annex L, and Annex M. If an Annex operating mode is not chosen, Annex A, Annex L, and Annex M are enabled. The final mode is decided by negotiation with the DSL access multiplexer (DSLAM).
		adsl2+—Configures operation in ADSL2+ mode-ITU G.992.5 Annex A and AnnexM. If an Annex A operating mode is not chosen, both Annex and Annex M is enabled. The final mode is decided by negotiation with DSLAM.
		ansi—Configures a router to operate in ANSI full-rate mode-ANSI T1.413.
		auto—Default setting. Configures the router so that the DSLAM automatically picks the DSL operating mode, in the sequence described in the "Usage Guidelines" section. All supported modes are enabled.
		vdsl2—Configures operation in ITU G.993.2 mode.
		annex a, m—(Optional) If the annex option is not specified, both Annex A and Annex M are enabled. The final mode is decided by negotiation with the Digital Synchronous Line Access Multiplexer (DSLAM).

Enabling Seamless Rate Adaption

To enable SRA, perform the following steps.

Note SRA mode is disabled by default.

Note SRA requires Cisco IOS Release 15.2(1)T or a later release.

Note These features are not currently available on the Cisco 866VAE, 867VAE, 866VAE-K9, or 867VAE-K9.

SUMMARY STEPS

SRA can be enabled and disabled with the following steps:

1. **enable**
2. **configure terminal**
3. **controller vdsl** *x/y/z*
4. **sra**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router# enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**controller vdsl** *x/y/z* **Example:** `Router(config)# controller vdsl 0/0/0`	Enters controller configuration mode. Use the controller vdsl command in global configuration mode. This command does not have a no form. *x*—Defines the network module. *y*—Defines the slot number. *z*—Defines the port number.
Step 4	**sra** **Example:** `router(config-controller)# sra`	Enables SRA mode. Use the no form of the command to disable SRA.

Seamless Rate Adaption Example

The following example enables SRA on a VDSL line:

```
!
!
!
rotuer>enable
router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
router(config)# controller vdsl 0
router(config-controller)# sra
router(config-controller)# end
router#
!
!
!
```

Configuring UBR+

Perform the following steps to configure UBR+.

Note Cisco IOS Release 15.2(1)T or a later release is required to run UBR+ on Cisco 886VA, 887VA, and 887VA-M routers.

Note These features are not currently available on the Cisco 866VAE, 867VAE, 866VAE-K9, or 867VAE-K9.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ubr+** *output-pcr output-mcr* [**input-pcr**] [**input-mcr**]

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`ubr+ output-pcr output-mcr [input-pcr] [input-mcr]`
	Example:
	`Router(config-if-vc)# ubr+ 10000 3000 9000 1000`
		Configures unspecified bit rate (UBR) quality of service (QoS) and specifies the output peak cell rate and output minimum guaranteed cell rate for an ATM permanent virtual circuit (PVC), PVC range, switched virtual circuit (SVC), virtual circuit (VC) class, or VC bundle member.
		To remove the UBR+ parameters, use the **no** form of this command.
		output-pcr—The output peak cell rate (PCR) in kbps.
		output-mcr—The output minimum guaranteed cell rate in kbps.
		input-pcr—(Optional for SVCs only) The input PCR in kbps. If this value is omitted, the input-pcr equals the output-pcr.
		input-mcr—(Optional for SVCs only) The input minimum guaranteed cell rate in kbps. If this value is omitted, the input-mcr equals the output-mcr.

UBR+ Example

The following example configures UBR+ PVC on a DSL line:

```
interface atm 0/0
 pvc 4/100
  ubr+ 2304 2304
```

The following example specifies the output-pcr argument for an ATM PVC to be 100000 kbps and the output-mcr to be 3000 kbps:

```
pvc 1/32
 ubr+ 100000 3000
```

The following example specifies the output-pcr, output-mcr, input-pcr, and input-mcr arguments for an ATM SVC to be 10000 kbps, 3000 kbps, 9000 kbps, and 1000 kbps, respectively:

```
svc lion nsap 47.0091.81.000000.0040.0B0A.2501.ABC1.3333.3333.05
 ubr+ 10000 3000 9000 1000
```

Troubleshooting

There are no new commands for checking traffic on the Cisco 886VA and 887VA. Some helpful commands include the following **show** commands:

- **show interface Ethernet0**
- **show interface ATM0**
- **show interface summary**
- **show controller vdsl 0**
- **show controller atm0**
- **show controller vdsl 0 datapath**
- **show atm pvc**

The "Cisco 860, Cisco 880, and Cisco 890 Series Integrated Services Routers Software Configuration Guide, Troubleshooting" section may also be helpful.

Configuring the Training Log Using the CLI

When you initiate the training log capture using the **debug vdsl 0 training log** on the Cisco 866VAE, Cisco 867VAE, Cisco 866VAE-K9, and Cisco 867VAE-K9 ISRs, the training log file opens. Any messages that are generated are buffered locally and are written to the training log file at 5k bytes per interval. The messages are not written all at one time, as in previous software versions that supported the training log capture feature.

Note A maximum log capacity of 8MB (approximately 1 hour of capture) exists on the Cisco 866VAE, Cisco 867VAE, Cisco 866VAE-K9, and Cisco 867VAE-K9 ISRs. Because of this capacity limitation, when the entire log collection exceeds 8MB, the log capture is automatically terminated.

Note Cisco 866VAE, Cisco 867VAE, Cisco 866VAE-K9, and Cisco 867VAE-K9 ISRs do not support the continuous training log autostop feature.

Capturing the Training Log

By default the training log is saved to `flash:vdsllog.bin`.

To start the training log capture, use the **debug vdsl 0 training log** command.

```
Router# debug vdsl 0 training log
Router#
```

The following confirmation is displayed:

```
Training log generation started for VDSL 0
```

Halting the Training Log Capture

To stop the training log capture, use the **no debug vdsl 0 training log** command.

```
Router# no debug vdsl 0 training log
Router#
```

The following confirmation is displayed:

```
Training Log file for VDSL written to flash:vdsllog.bin
```

Displaying the Training Log Status and File Location

To display the training log status and file location, use the **show controller vdsl 0** command.

```
Router# show controller vdsl 0
Router#
```

The following confirmation is displayed:

```
Controller VDSL 0 is UP

Daemon Status:           NA

                        XTU-R (DS)              XTU-C (US)
Chip Vendor ID:         'BDCM'                   'BDCM'
Chip Vendor Specific:   0x0000                   0x938C
Chip Vendor Country:    0xB500                   0xB500
Modem Vendor ID:        'CSCO'                   'BDCM'
Modem Vendor Specific:  0x4602                   0x938C
Modem Vendor Country:   0xB500                   0xB500
Serial Number Near:    GMH1049001M 867VAE-K 15.1(20110
Serial Number Far:
Modem Version Near:    15.1(20110422:230431) [suguraja
Modem Version Far:     0x938C

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:          0.0 dB                  0.0 dB
Signal Attenuation:        0.0 dB                  0.0 dB
Noise Margin:            16.0 dB                 14.6 dB
Attainable Rate:        28516 kbits/s            1222 kbits/s
Actual Power:             7.0 dBm                12.4 dBm
Total FECS:             3                        0
Total ES:               0                        0
Total SES:              0                        0
Total LOSS:             0                        0
Total UAS:              147                      147
Total LPRS:             0                        0
Total LOFS:             0                        0
Total LOLS:             0                        0
Bit swap:               0                        0

Full inits:             1
Failed full inits:      0
Short inits:            0
Failed short inits:     0

Firmware        Source          File Name (version)
--------        ------          -------------------
VDSL            embedded         (0)

Modem FW  Version:      23a
Modem PHY Version:      A2pv6C032b.d23a


                  DS Channel1     DS Channel0   US Channel1       US Channel0
Speed (kbps):             0            24543             0              1020
Previous Speed:           0                0             0                 0
Total Cells:              0         87837567             0           3652502
User Cells:               0                0             0                 0
Reed-Solomon EC:          0                3             0                 0
CRC Errors:               0                0             0                 0
Header Errors:            0                0             0                 0
Interleave (ms):       0.00            15.00          0.00              3.76
Actual INP:            0.00            57.00          0.00              0.50

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

Configuring a G.SHDSL WAN Interface in ATM mode

Perform the following steps to configure G.SHDSL on the Cisco 888 ISR perform these steps, beginning in global configuration mode.

SUMMARY STEPS

1. **controller dsl** *slot/port*
2. **mode atm**
3. **line-term cpe**
4. **line-mode 4 wire standard**
5. **line-rate** {**auto** | *rate*}

6. **interface atm** *interface-number*
7. **ip-address** *ip-address*
8. **load-interval** *seconds*
9. **no atm ilmi-keepalive** [*seconds*]
10. **pvc** [*name*] *vpi/vci*
11. **protocol** *protocol protocol-address* **broadcast**
12. **encapsulation** *encapsulation-type*

DETAILED STEPS

	Command	Purpose
Step 1	**controller dsl** *slot/port* **Example:** `Router(config)# controller dsl 0`	Enters controller configuration mode and the controller number.
Step 2	**mode atm** **Example:** `Router(config-ctrl)# mode atm`	Enables ATM encapsulation and creates logical ATM interface 0.
Step 3	**line-term cpe** **Example:** `Router(config-ctrl)# line-term cpe`	Enables CPE.
Step 4	**line-mode 4 wire standard** **Example:** `Router(config-ctrl)# line-mode 4 wire standard`	Enables 4 wire operation.

Step 5	**line-rate** {**auto** | *rate*}
	Example:
	`Router(config-ctrl)# line-rate 4608`
		Specifies the DSL line rate for the SHDSL port. The range is 192 to 2312 kbps. The default is **auto** (negotiated between the SHDSL port and the DSLAM).
		Note If different DSL line rates are configured at opposite ends of the DSL uplink, the actual DSL line rate is always the lower rate.
		Note The maximum peak cell rate is 8 kbps less than the line rate.

Step 6	**interface atm** *interface-number* **Example:** `Router(config-ctrl)# interface atm0`	Enters ATM configuration mode for interface ATM 0.

	Command	Purpose
Step 7	**ip-address** *ip-address* **Example:** `Router(config-ctrl)# ip-address IP-address`	Assigns an IP address to the DSL ATM interface.
Step 8	**load-interval** *seconds* **Example:** `Router(config-ctrl)# load-interval 3`	Assigns a load interval value.
Step 9	**no atm ilmi-keepalive** [*seconds*] **Example:** `Router(config-ctrl)# no atm ilmi-keepalive0`	Disables Integrated Local Management Interface (ILMI) keepalives. If you enable ILMI keepalives without specifying the number of seconds, the default time interval is 3 seconds.
Step 10	**pvc** [*name*] *vpi/vci* **Example:** `Router(config-ctrl)# pvc 0/35`	Enters atm-virtual-circuit (interface-atm-vc) configuration mode, and configures a new ATM PVC by assigning a name (optional) and VPI/VCI numbers. The default traffic shaping is UBR; the default encapsulation is AAL5+LLC/SNAP.
Step 11	**protocol** *protocol protocol-address* **broadcast** **Example:** `Router(config-ctrl)# protocol ip 10.10.10.2 broadcast`	Enables IP connectivity and creates a point-to-point IP address for the VC.
Step 12	**encapsulation** [*encapsulation-type*] **Example:** `Router(config-ctrl)# encapsulation aal5snap`	Configures the ATM adaptation layer (AAL) and encapsulation type. • Use the **aal2** keyword for AAL2 • Use the **aal5ciscoppp** keyword for Cisco PPP over AAL5 • Use the **aal5mux** keyword for AAL5+MUX • Use the **aal5nlpid** keyword for AAL5+NLPID • Use the **aal5snap** keyword for AAL5+LLC/SNAP (the default)

Example

The following configuration example shows a 4-wire standard G.SHDSL configuration.

```
!
controller DSL 0
 mode atm
 line-term cpe
 line-mode 4-wire standard
 dsl-mode shdsl symmetric annex B
 line-rate 4608
!
interface BRI0
 no ip address
 encapsulation hdlc
 shutdown
 isdn termination multidrop
!
!
interface ATM0
 ip address 10.10.10.1 255.255.255.0
 no atm ilmi-keepalive
 pvc 0/35
  protocol ip 10.10.10.2 broadcast
  encapsulation aal5snap
 !
!
interface FastEthernet0
!
interface FastEthernet1
!
interface FastEthernet2
!
interface FastEthernet3
 shutdown
!
interface Vlan1
 ip address 2.15.15.26 255.255.255.0
!
ip forward-protocol nd
ip route 223.255.254.254 255.255.255.255 Vlan1
no ip http server
no ip http secure-server
!
```

Verifying Configuration

To verify that you have properly configured the router, enter the **show running** command and look for controller DSL and interface ATM0 parameters.

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

Current configuration : 1298 bytes
!
.......

!
controller DSL 0
 mode atm
 line-term cpe
 line-mode 4-wire standard
 dsl-mode shdsl symmetric annex B
 line-rate 4608
!
!
interface ATM0
 ip address 10.10.10.1 255.255.255.0
 no atm ilmi-keepalive
 pvc 0/31
  protocol ip 10.10.10.5 broadcast
  encapsulation aal5snap
 !
```

Configuring a G.SHDSL WAN Interface in EFM mode

To configure G.SHDSL on the Cisco 888E ISR, perform Configuring Cisco G.SHDSL EFM HWICs in Cisco Routers at:

http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/GSHDSL_EFM_HWICS.html

Configuring the Cellular Wireless WAN Interface

The Cisco 880 series ISRs provide a third generation (3G) wireless interface for use over Global System for Mobile Communications (GSM) and code division multiple access (CDMA) networks. The interface is a 34-mm PCMCIA slot.

Its primary application is WAN connectivity as a backup data link for critical data applications. However, the 3G wireless interface can also function as the primary WAN connection for the router.

To configure the 3G cellular wireless interface, follow these guidelines and procedures:

- Prerequisites for Configuring the 3G Wireless Interface, page 3-41
- Restrictions for Configuring the Cellular Wireless Interface, page 3-42
- Data Account Provisioning, page 3-42
- Configuring a Cellular Interface, page 3-46
- Configuring DDR, page 3-48
- Configuring Data Dedicated Transmission Mode (DDTM), page 3-50
- Examples for Configuring Cellular Wireless Interfaces, page 3-50

Prerequisites for Configuring the 3G Wireless Interface

The following are prerequisites to configuring the 3G wireless interface:

- You must have wireless service from a carrier, and you must have network coverage where your router will be physically placed. For a complete list of supported carriers, see the data sheet at:

  http://www.cisco.com/en/US/prod/routers/networking_solutions_products_genericcontent0900aecd80601f7e.html

- You must subscribe to a service plan with a wireless service provider and obtain a SIM card (GSM modem only) from the service provider.
- You must check your LEDs for signal strength, as described in Table 3-2.
- You should be familiar with the Cisco IOS software, beginning with Cisco NX-OS Release 4.1 or later. For Cisco 3G Wireless support, see the Cisco IOS documentation.
- To configure your GSM data profile, you need the following information from your service provider:
  - Username
  - Password
  - Access point name (APN)
- To configure your CDMA data profile for manual activation, you need the following information from your service provider:
  - Master Subsidy Lock (MSL) number
  - Mobile Directory number (MDN)
  - Mobile Station Identifier (MSID)
  - Electronic Serial Number (ESN)

Table 3-2 Front Panel LED Signal Strength Indications

LED	LED Color	Signal Strength
P3G RSSI[1]	Amber	No service available and no RSSI detected
	Solid green	High RSSI (–69 dBm or higher)
	Fast (16 Hz) blinking green	Medium RSSI (–89 to –70 dBm)
	Slow (1 Hz) blinking green	Low to medium RSSI (–99 to –90 dBm), minimum level for a reliable connection
	Off	Low RSSI (less than –100 dBm)

[1] 3G RSSI = 3G receive signal strength indication.

Restrictions for Configuring the Cellular Wireless Interface

The following restrictions apply to configuring the Cisco 3G wireless interface:

- A data connection can be originated only by the 3G wireless interface. Remote dial-in is not supported.
- Because of the shared nature of wireless communications, the experienced throughput varies depending on the number of active users or the amount of congestion in a given network.
- Cellular networks have higher latency than wired networks. Latency rates depend on the technology and carrier. Latency may be higher when there is network congestion.
- VoIP is not currently supported.
- Any restrictions that are part of the terms of service from your carrier also apply to the Cisco 3G wireless interface.
- Cisco 880G ISR does not support online insertion and removal (OIR) of 3G modems. To replace a modem with another modem of the same type, use the Cisco CLI to enter the **shutdown** command on the cellular interface before you replace the modems. =
- When a 3G modem is removed, the **show interface cellular 0**, **show run**, and **show version** command outputs still display cellular interface related information. The **show interface** command displays the following message, all other show commands have empty outputs.

  ```
  3G Modem not inserted
  ```

- You can configure the cellular interface when the 3G modem is removed. However, the configuration is not effective until the 3G modem is inserted. The following message is shown when trying to configure the cellular interface while the modem is absent.

  ```
  Router(config)# interface cellular 0
  Warning: 3G Modem is not inserted
  Configuration will not be effective until modem is inserted =
  ```

- Inserting a different type of modem than was previously removed requires configuration changes and you must reload the system.

Data Account Provisioning

Note To provision your modem, you must have an active wireless account with a service provider. A SIM card must be installed in a GSM 3G wireless card.

To provision your data account, follow these procedures:

- Verifying Signal Strength and Service Availability, page 3-43
- Configuring a GSM Modem Data Profile, page 3-44
- CDMA Modem Activation and Provisioning, page 3-45

Verifying Signal Strength and Service Availability

To verify the signal strength and service availability on your modem, use the following commands in privileged EXEC mode.

SUMMARY STEPS

1. **show cellular 0 network**
2. **show cellular 0 hardware**
3. **show cellular 0 connection**
4. **show cellular 0 radio**
5. **show cellular 0 profile**
6. **show cellular 0 security**
7. **show cellular 0 all**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show cellular 0 network** **Example:** `Router# show cellular 0 network`	Displays information about the carrier network, cell site, and available service.
Step 2	**show cellular 0 hardware** **Example:** `Router# show cellular 0 hardware`	Displays the cellular modem hardware information.
Step 3	**show cellular 0 connection** **Example:** `Router# show cellular 0 connection`	Displays the current active connection state and data statistics.
Step 4	**show cellular 0 radio** **Example:** `Router# show cellular 0 radio`	Shows the radio signal strength. **Note** The RSSI should be better than –90 dBm for steady and reliable connection.
Step 5	**show cellular 0 profile** **Example:** `Router# show cellular 0 profile`	Shows information about the modem data profiles created.

	Command or Action	Purpose
Step 6	**show cellular 0 security** **Example:** `Router# show cellular 0 security`	Shows the security information for the modem, such as SIM and modem lock status.
Step 7	**show cellular 0 all** **Example:** `Router# show cellular 0 all`	Shows consolidated information about the modem. The profiles that were created, the radio signal strength, the network security, and so on.

Configuring a GSM Modem Data Profile

To configure or create a new modem data profile, enter the **cellular 0 gsm profile create** <*profile number*> <*apn*> <*authentication*> <*username*> <*password*> command in privileged EXEC mode. See Table 3-3 for details about the command parameters.

Example

```
Router# cellular 0 gsm profile create 3 apn.com chap GSM GSMPassword
```

Table 3-3 lists the modem data profile parameters.

Table 3-3 Modem Data Profile Parameters

profile number	Number for the profile that you are creating. You can create up to 16 profiles.
apn	Access point name. You must get this information from your service provider.
authentication	Type of authentication, for example, CHAP, PAP.
username	Username provided by your service provider.
password	Password provided by your service provider.

CDMA Modem Activation and Provisioning

Activation procedures may differ, depending upon your carrier. Consult your carrier, and perform one of the following procedures as appropriate:

- Manual activation
- Activation using over the air service provisioning

Table 3-4 lists the activation and provisioning processes supported by different wireless carriers.

Table 3-4 CDMA Modem Activation and Provisioning

Activation and Provisioning Process	Carrier
Manual Activation using MDN, MSID, MSL	Sprint
OTASP[1] Activation	Verizon Wireless
IOTA[2] for Data Profile refresh	Sprint

[1] OTASP = Over the Air Service Provisioning.

[2] IOTA = Internet Over the Air.

Manual Activation

Note You must have valid mobile directory number (MDN), mobile subsidy lock (MSL), and mobile station identifier (MSID) information from your carrier before you start this procedure.

To configure a modem profile manually, use the following command, beginning in EXEC mode:

cellular 0 cdma activate manual mdn msid sid nid msl

Besides being activated, the modem data profile is provisioned through the Internet Over the Air (IOTA) process. The IOTA process is initiated automatically when you use the **cellular cdma activate manual** command.

The following is a sample output from this command:

```
router# cellular 0 cdma activate manual 1234567890 1234567890 1234 12 12345
NAM 0 will be configured and will become Active
Modem will be activated with following Parameters
MDN :1234567890; MSID :1234567890; SID :1234; NID 12:
Checking Current Activation Status
Modem activation status: Not Activated
Begin Activation
Account activation - Step 1 of 5
Account activation - Step 2 of 5
Account activation - Step 3 of 5
Account activation - Step 4 of 5
Account activation - Step 5 of 5
Secure Commit Result: Succeed
Done Configuring - Resetting the modem
The activation of the account is Complete
Waiting for modem to be ready to start IOTA
Beginning IOTA
router#
*Feb  6 23:29:08.459: IOTA Status Message Received. Event: IOTA Start, Result: SUCCESS
*Feb  6 23:29:08.459: Please wait till IOTA END message is received
*Feb  6 23:29:08.459: It can take up to 5 minutes
*Feb  6 23:29:27.951: OTA State = SPL unlock, Result = Success
*Feb  6 23:29:32.319: OTA State = Parameters committed to NVRAM, Result = Success
```

```
*Feb  6 23:29:40.999: Over the air provisioning complete; Result:Success
*Feb  6 23:29:41.679: IOTA Status Message Received. Event: IOTA End, Result: SUCCESS
```

The IOTA start and end must have “success” as the resulting output. If you receive an error message, you can run IOTA independently by using the **cellular cdma activate iota** command.

Your carrier may require periodic refreshes of the data profile. Use the following command to refresh the data profile:

cellular cdma activate iota

Activating with Over-the-Air Service Provisioning

To provision and activate your modem using Over-the-Air Service Provisioning (OTASP), use the following command, beginning in EXEC mode.

router # **cellular 0 cdma activate otasp** *phone_number*

Note You need to obtain the phone number for use with this command from your carrier. The standard OTASP calling number is *22899.

The following is a sample output from this command:

```
router# cellular 0 cdma activate otasp  *22899
Beginning OTASP activation
OTASP number is *22899
steelers_c881G#
OTA State = SPL unlock, Result = Success
router#
OTA State = PRL downloaded, Result = Success
OTA State = Profile downloaded, Result = Success
OTA State = MDN downloaded, Result = Success
OTA State = Parameters committed to NVRAM, Result = Success
Over the air provisioning complete; Result:Success
```

Configuring a Cellular Interface

To configure the cellular interface, enter the following commands, beginning in privileged EXEC mode.

SUMMARY STEPS

1. **configure terminal**
2. **interface cellular 0**
3. **encapsulation ppp**
4. **ppp chap hostname** *host*
5. **ppp chap password 0** *password*
6. **asynchronous mode interactive**
7. **ip address negotiated**

Note The PPP Challenge Handshake Authentication Protocol (CHAP) authentication parameters that you use in this procedure must be the same as the username and password provided by your carrier and configured only under the GSM profile. CDMA does not require a username or password.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode from the terminal.
Step 2	**interface cellular 0** **Example:** `Router (config)# interface cellular 0`	Specifies the cellular interface.
Step 3	**encapsulation ppp** **Example:** `Router (config-if)# encapsulation ppp`	Specifies PPP encapsulation for an interface configured for dedicated asynchronous mode or dial-on-demand routing (DDR).
Step 4	**ppp chap hostname** *host* **Example:** `Router (config-if)# ppp chap hostname host@wwan.ccs`	Defines an interface-specific Challenge Handshake Authentication Protocol (CHAP) hostname. This must match the username given by the carrier. Applies to GSM only.
Step 5	**ppp chap password 0** *password* **Example:** `Router (config-if)# ppp chap password 0 cisco`	Defines an interface-specific CHAP password. This must match the password given by the carrier.
Step 6	**asynchronous mode interactive** **Example:** `Router (config-if)# asynchronous mode interactive`	Returns a line from dedicated asynchronous network mode to interactive mode, enabling the **slip** and **ppp** commands in privileged EXEC mode.
Step 7	**ip address negotiated** **Example:** `Router (config-if)# ip address negotiated`	Specifies that the IP address for a particular interface is obtained via PPP and IPCP address negotiation.

Note When the cellular interface requires a static IP address, the address may be configured as **ip address negotiated**. Through IP Control Protocol (IPCP), the network ensures that the correct static IP address is allocated to the device. If a tunnel interface is configured with the **ip address unnumbered** *cellular interface* command, the actual static IP address must be configured under the cellular interface, in place of **ip address negotiated**. For a sample cellular interface configuration, see the "Basic Cellular Interface Configuration" section on page 3-50.

Configuring DDR

Perform these steps to configure dial-on-demand routing (DDR) for the cellular interface.

SUMMARY STEPS

1. **configure terminal**
2. **interface cellular 0**
3. **dialer in-band**
4. **dialer idle-timeout** *seconds*
5. **dialer string** *string*
6. **dialer group** *number*
7. **exit**
8. **dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | **access-group**}
9. **ip access-list** *access list number* **permit** *ip source address*
10. **line 3**
11. **script dialer** *regexp*
12. **exit**
13. **chat-script** *script name* **”” “ATDT*99***profile number***#” TIMEOUT** *timeout value* **CONNECT**
or
chat-script *script name* "" **"ATDT*777***profile number***#" TIMEOUT** *timeout value* **CONNECT**
14. **interface cellular 0**
15. **dialer string** *string*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**interface cellular 0** **Example:** `Router (config)# interface cellular 0`	Specifies the cellular interface.
Step 3	**dialer in-band** **Example:** `Router (config-if)# dialer in-band`	Enables DDR and configures the specified serial interface for in-band dialing.

	Command or Action	Purpose
Step 4	**dialer idle-timeout** *seconds* **Example:** `Router (config-if)# dialer idle-timeout 30`	Specifies the duration of idle time, in seconds, after which a line is disconnected.
Step 5	**dialer string** *string* **Example:** `Router (config-if)# dialer string gsm`	Specifies the number or string to dial. Use the name of the chat script here.
Step 6	**dialer-group** *number* **Example:** `Router (config-if)# dialer-group 1`	Specifies the number of the dialer access group to which a specific interface belongs.
Step 7	**exit** **Example:** `Router (config-if)# exit`	Enters the global configuration mode.

Step 8	**dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | **access-group**}
	Example:
	`Router (config)# dialer-list 1 protocol ip list 1`
		Creates a dialer list for traffic of interest and permits access to an entire protocol.

Step 9	**ip access-list** *access list number* **permit** *ip source address* **Example:** `Router (config)# ip access list 1 permit any`	Defines traffic of interest.
Step 10	**line 3** **Example:** `Router (config-line)# line 3`	Specifies the line configuration mode. It is always 3.
Step 11	**script dialer** *regexp* **Example:** `Router (config-line)# script-dialer gsm`	Specifies a default modem chat script.
Step 12	**exit** **Example:** `Router (config-line)# exit`	Exits line configuration mode.

	Command or Action	Purpose
Step 13	For GSM: **chat-script** *script name* **”” “ATDT*99*** *profile number***#”** **TIMEOUT** *timeout value* **CONNECT** For CDMA: **chat-script** *script name* "" **"ATDT*777*** *profile number***#"** **TIMEOUT** *timeout value* **CONNECT** **Example:** `Router (config)# chat-script gsm "" "ATDT*98*2#" TIMEOUT 60 "CONNECT‟`	Configures the line for GSM. Configures the line for CDMA. Defines the Attention Dial Tone (ATDT) commands when the dialer is initiated.
Step 14	**interface cellular 0** **Example:** `Router (config)# interface cellular 0`	Specifies the cellular interface.
Step 15	**dialer string** *string* **Example:** `Router (config)# dialer string gsm`	Specifies the dialer script (defined using the **chat script** command).

Configuring Data Dedicated Transmission Mode (DDTM)

On CDMA modems, data transmission is disrupted by incoming voice calls if data dedicated transmission mode (DDTM) is disabled. You can enable DDTM mode so the modem ignores incoming voice calls.

To enable DDTM on a CDMA modem, use the **cdma ddtm** command in configuration mode.

This command is enabled by default. You can disable this feature by using the **no cdma ddtm** command.

Note When DDTM is enabled, only voice calls are blocked for the MC5728v modems. On the AC597E and MC5725 and MC 5727, incoming SMS messages are also blocked.

Examples for Configuring Cellular Wireless Interfaces

This section provides the following configuration examples:

- Basic Cellular Interface Configuration, page 3-50
- Tunnel over Cellular Interface Configuration, page 3-51

Basic Cellular Interface Configuration

The following example shows how to configure a gsm cellular interface to be used as a primary WAN connection. It is configured as the default route.

```
chat-script gsm "" "ATDT*98*2#" TIMEOUT 60 "CONNECT‟

!
interface Cellular0
```

```
 ip address negotiated
 encapsulation ppp
 dialer in-band
 dialer string gsm
 dialer-group 1
 async mode interactive
 ppp chap hostname cisco@wwan.ccs
 ppp chap password 0 cisco
 ppp ipcp dns request
!

ip route 0.0.0.0 0.0.0.0 Cellular0
!
!
access-list 1 permit any
dialer-list 1 protocol ip list 1
!
line 3
 exec-timeout 0 0
 script dialer gsm
 login
 modem InOut
```

The following example shows how to configure a cdma cellular interface to be used as a primary. It is configured as the default route.

```
chat-script cdma "" "ATDT#777" TIMEOUT 60 "CONNECT‟

!
interface Cellular0
 ip address negotiated
 encapsulation ppp
 dialer in-band
 dialer string cdma
 dialer-group 1
 async mode interactive
 ppp chap password 0 cisco
!

ip route 0.0.0.0 0.0.0.0 Cellular0
!
!
access-list 1 permit any
dialer-list 1 protocol ip list 1
!
line 3
 exec-timeout 0 0
 script dialer cdma
 login
 modem InOut
```

Tunnel over Cellular Interface Configuration

The following example shows how to configure the static IP address when a tunnel interface is configured with the **ip address unnumbered** <*cellular interface*> command:

```
interface Tunnel2
 ip unnumbered Cellular0
 tunnel source Cellular0
 tunnel destination 128.107.248.254

interface Cellular0
```

```
 bandwidth receive 1400000
 ip address 23.23.0.1 255.255.0.0
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
 no ip mroute-cache
 dialer in-band
 dialer idle-timeout 0
 dialer string dial<carrier>
 dialer-group 1
 async mode interactive
 no ppp lcp fast-start
 ppp chap hostname <hostname>        *** gsm only ***
 ppp chap password 0 <password>
 ppp ipcp dns request
 ! traffic of interest through the tunnel/cellular interface
ip route 10.10.0.0 255.255.0.0 Tunnel2
```

Configuring WAN Mode on Cisco 860VAE ISRs

The Cisco 866VAE, Cisco 867VAE, Cisco 866VAE-K9, and Cisco 867VAE-K9 routers can be configured to use either a GE interface or a DSL interface as a WAN link. DSL is the default WAN interface when the Cisco 866VAE, Cisco 867VAE, Cisco 866VAE-K9, and Cisco 867VAE-K9 routers boot.

After the router boots up, the desired WAN interface can be selected using the **wan mode** command. When WAN mode is configured as Ethernet, both ATM0 and Ethernet0 interfaces will be forced into shutdown state. Entering the **no shutdown** command on either of the DSL interfaces will be rejected with a message ***WAN interface is Ethernet***. Similarly, when the WAN mode is DSL, the GE WAN interface will be put in shutdown state and the **no shutdown** command will be rejected with the message ***WAN interface is DSL***.

Note The routers do not support enabling both GE and DSL interfaces simultaneously.

Use the **wan mode dsl | ethernet** command to switch from DSL to Ethernet interfaces or vice versa.

This section contains the following information:

- Enabling WAN Mode, page 3-52
- Displaying WAN Mode Configuration, page 3-53

Enabling WAN Mode

Perform the following steps to select and enable WAN mode.

SUMMARY STEPS

1. **enable**
2. **show running-configuration**
3. **wan mode {dsl | ethernet}**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show running-configuration** **Example:** `Router# show running-configuration`	Displays the default entries on boot up.

Step 3	**wan mode {dsl | ethernet}**
	Example:
	`Router(config)# wan mode dsl`
		Selects the desired WAN mode.

Step 4	**exit**
	Example:
	`Router(config)# exit`
	`Router#`
		Exits configuration mode and returns to it would take the router back to privileged EXEC mode.

Displaying WAN Mode Configuration

Use the **show running-config** command to view the initial configuration, as shown in the following example for a Cisco 866VAE router.

Note Your Cisco router displays the WAN mode during the boot sequence after the initial configuration is complete.

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

Current configuration : 1195 bytes
!
! Last configuration change at 13:27:25 UTC Wed Feb 24 2010
version 15.2
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
enable password lab
!
no aaa new-model
wan mode ethernet
```

```
no ipv6 cef
!
!
!
!
!
ip cef
!
crypto pki token default removal timeout 0
!
!
!
!
!
!
controller VDSL 0
 shutdown
!
!
!
!
!
interface ATM0
 no ip address
 shutdown
 no atm ilmi-keepalive
!
interface ATM0.1 point-to-point
 ip address 202.0.0.1 255.255.255.0
 pvc 0/202
 !
!
interface Ethernet0
 no ip address
 shutdown
!
interface FastEthernet0
 no ip address
!
interface FastEthernet1
 no ip address
!
interface FastEthernet2
 no ip address
!
interface FastEthernet3
 no ip address
!
interface GigabitEthernet0
 ip address 1.0.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
!
control-plane
```

```
!
!
line con 0
 exec-timeout 0 0
 no modem enable
line aux 0
line vty 0 4
 login
 transport input all
!
scheduler allocate 60000 1000
!
end

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 can also assign the interfaces to other VLANs. For more information about creating VLANs, see Chapter 7, "Configuring Ethernet Switches."

Configuring the Wireless LAN Interface

The Cisco 860, Cisco 880, and Cisco 890 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 Chapter 9, "Basic Wireless Device Configuration."

Configuring a Loopback Interface

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

Perform these steps to configure a loopback interface, 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** *loopback number*
	Example:
	`Router(config)# interface Loopback 0`
	`Router(config-if)#`
		Enters configuration mode for the loopback interface.
		number—number of the loopback interface.

Step 2	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.108.1.1 255.255.255.0`	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 verification output similar to the following example.

```
Router# show interface loopback 0
Loopback 0 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.

Follow these steps to configure static routes, 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`
		Specifies the static route for the IP packets.
		For details about this command and about additional parameters that can be set, see the *Cisco IOS IP Routing Protocols Command Reference*.

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

For general information on static routing, see the "Concepts" section on page B-1

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 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 3-59
- Configuring Enhanced Interior Gateway Routing Protocol, page 3-60

Configuring Routing Information Protocol

To configure the RIP routing protocol on the router, perform 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(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`
			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`
		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`	Disables automatic summarization of subnet routes into network-level routes. This allows subprefix routing information to pass across classfull network boundaries.

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

For general information on RIP, see the "RIP" section on page B-3

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 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 Enhanced Interior Gateway Routing Protocol (EIGRP), perform 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`	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.

	Command	Purpose

Step 2	**network** *ip-address*
	Example:
	`Router(config)# network 192.145.1.0`
	`Router(config)# network 10.10.12.115`
		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.

For general information on EIGRP concepts, see the "Enhanced IGRP" section on page B-3

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 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

Configuring Ethernet CFM and Y.1731 Performance Monitoring on Layer 3 Interfaces

This chapter provides procedures for configuring the network interface device functionality, Ethernet data plane loopback, IEEE connectivity fault management, and Y.1731 performance monitoring, and contains the following sections:

Configuring a Network Interface Device on the L3 Interface

Configuring a Network Interface Device (NID) enables support for the NID functionality on the router without including a NID hardware in the network. This feature combines the Customer-Premises Equipment (CPE) and the NID functionality into a physical device. The following are the advantages of configuring the NID functionality:

- Eliminates a physical device.
- Supports both the managed CPE feature set and the NID requirements.

Note This feature is supported only if you have purchased the *advipservices* licensing module. For more information about managing software activation licenses on the Cisco ISR and Cisco ISR G2 platforms, see http://www.cisco.com/en/US/docs/routers/access/sw_activation/SA_on_ISR.html.

Configuring the NID

The following steps describe how to configure the NID:

SUMMARY STEPS

Step 1 **enable**

Step 2 **configure terminal**

Step 3 **interface gigabitethernet** *slot/port*

Step 4 **port-tagging**

Step 5 **encapsulation dot1q** *vlan-id*

Step 6 **set cos** *cos-value*

Step 7 **end**

DETAILED STEPS

	Command	Purpose

Step 1	**`enable`**
	Example:
	`Router>enable`
		Enables the privileged EXEC mode.
		Enter your password when prompted.

Step 2	**`configure terminal`**
	Example:
	`Router#configure terminal`
		Enters the global configuration mode.

Step 3	**`interface gigabitethernet`** *`slot/port`*
	Example:
	`Router(config)#interface gigabitethernet 0/2`
		Specifies an interface and enters the interface configuration mode.

Step 4	**`port-tagging`**
	Example:
	`Router(config-if)#port-tagging`
		Inserts the VLAN ID into a packet header to identify which Virtual Local Area Network (VLAN) the packet belongs to.

Step 5	**`encapsulation dot1q`** *`vlan-id`*
	Example:
	`Router(config-if-port-tagging)#encapsulation dot1q 10`
		Defines the encapsulation format as IEEE 802.1Q (dot1q), and specifies the VLAN identifier.

Step 6	**`set cos`** *`cos-value`*
	Example:
	`Router(config-if-port-tagging)#set cos 6`
		Sets the Layer 2 class of service (CoS) value to an outgoing packet end.

Step 7	**`end`**
	Example:
	`Router(config-if-port-tagging)#end`
		Exits the interface configuration mode.

Configuration Example

This configuration example shows how to configure the NID:

```
Router>enable
```

```
Router#configure terminal
Router(config)#interface gigabitethernet 0/2
Router(config-if)#port-tagging
Router(config-if-port-tagging)#encapsulation dot1q 10
Router(config-if-port-tagging)#set cos 6
Router(config-if-port-tagging)#end
```

Verifying the NID Configuration

Use the following commands to verify the port tagging sessions:

- **show run int**
- **ping**

Use the **show run int** command to display the port tagging sessions:

```
Router#show run int gi0/2
Building configuration...
Current configuration : 10585 bytes
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 port-tagging
  encapsulation dot1q 10
  set cos 6
  exit
end
!
interface GigabitEthernet0/2.1101
encapsulation dot1Q 100
ip address 132.1.101.4 255.255.255.0
!
interface GigabitEthernet0/2.1102
encapsulation dot1Q 100
ip address 132.1.102.4 255.255.255.0
!
```

Use the **ping** command to verify the connectivity with port tagging configured:

```
Router#ping 132.1.101.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 132.1.101.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
router#
```

Troubleshooting the NID Configuration

Table 4-1 lists the debug commands to troubleshoot the issues pertaining to the NID functionality.

The Cisco IOS Master Command List at

http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html provides more information about these commands.

Caution Because debugging output is assigned high priority in the CPU process, it can diminish the performance of the router or even render it unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff.

Note Before you run any of the debug commands listed in the following table, ensure that you run the **logging buffered debugging** command, and then turn off console debug logging using the **no logging console** command.

Table 4-1 debug Commands for NID Configuration

debug Command	Purpose
debug ethernet nid configuration	Enables debugging of configuration-related issues.
debug ethernet nid packet egress	Enables debugging of packet processing (VLAN tag push) on the egress side.
debug ethernet nid packet ingress	Enables debugging of packet processing (VLAN tag pop) on the ingress side.

Ethernet Data Plane Loopback

The Ethernet Data Plane Loopback feature provides a means for remotely testing the throughput of an Ethernet port. You can verify the maximum rate of frame transmission with no frame loss.

Note This feature is supported only if you have purchased the *advipservices* licensing module. For more information about managing software activation licenses on the Cisco ISR and Cisco ISR G2 platforms, see http://www.cisco.com/en/US/docs/routers/access/sw_activation/SA_on_ISR.html.

Note Internal Ethernet data plane loopback is not supported.

Restrictions for Configuring Ethernet Data Plane Loopback

Follow the guidelines and take note of the restrictions listed here when configuring Ethernet data plane loopback on a Layer 3 interface:

- Only external loopback (packets coming from the wire side) on the L3 dot1q subinterface and (untagged) main interface are supported.
- To perform a MAC swap, the destination address and source address must be swapped for the packets that are looped back. If the destination address is broadcast or multicast, the MAC address is used as the source address for the packets that are looped back.
- Loopback operations are supported at line rate.
- Untagged frames are not supported on a subinterface. However, the frames for *dot1q* and *qinq* are supported on a subinterface.
- *dot1ad* is not supported on the main interface. However, untagged frames are supported on the main interface.
- Single VLAN is supported as a filtering option for a subinterface, but VLAN list and VLAN range are not supported.
- Only MAC address is supported as a filtering option for the main interface.

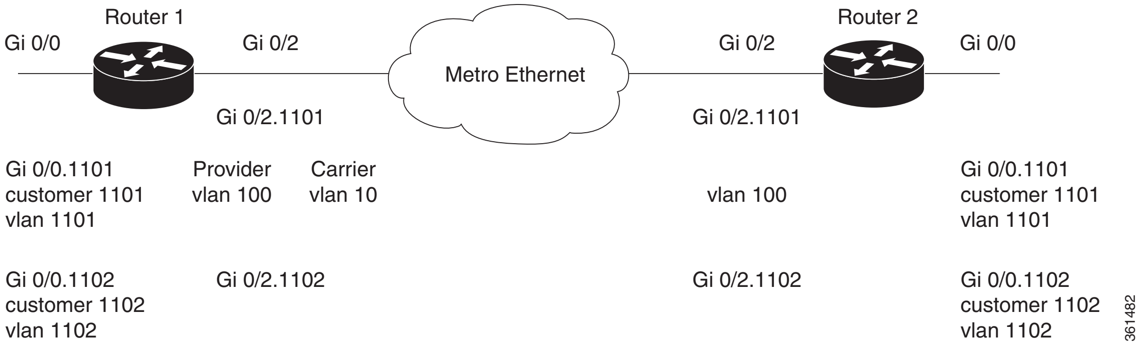
- For the filtering option, the destination MAC cannot be combined with inner VLAN or outer VLAN.
- There is no support for L3 and L4 loopback. Source and destination IP address or source and destination ports will not be swapped.
- Connectivity Fault Management (CFM) packets are transparent to the data plane loopback configuration and cannot be looped back.
- Packets coming from the other side of the wire where loopback is configured and having the same destination MAC address are dropped.
- The broadcast and multicast IP addresses of the broadcast and multicast IP frames that are received cannot be used as the source IP address of the frame when it is sent back to the initiator. In such a case, the IP address of the subinterface is used as the source IP address of the frame when it is sent back to the initiator.

Configuring External Ethernet Data Plane Loopback

Configuring external Ethernet data plane loopback is permitted on a Layer 3 main interface and subinterfaces.

Figure 4-1 represents a sample topology to configure Ethernet data plane loopback.

Figure 4-1 Sample Topology



The following steps show how to configure external Ethernet data plane loopback on a subinterface using single and double tagging. (The procedure to configure external Ethernet data plane loopback on the main interface is similar to this procedure.)

SUMMARY STEPS

Step 1 **enable**

Step 2 **configure terminal**

Step 3 **interface gigabitethernet** *slot/port.sub-port*

Step 4 **encapsulation dot1q** *vlan-id*

or

encapsulation dot1q *vlan-id* **second-dot1q** *inner vlan-id*

Step 5 **ethernet loopback permit external**

Step 6 **end**

DETAILED STEPS

	Command	Purpose

Step 1	**`enable`**
	Example:
	`Router>enable`
		Enables the privileged EXEC mode.
		Enter your password when prompted.

Step 2	**`configure terminal`**
	Example:
	`Router#configure terminal`
		Enters the global configuration mode.

Step 3	**`interface gigabitethernet`** *`slot/port.sub-port`*
	Example:
	`Router(config)#interface gigabitethernet 0/2.1101`
		Specifies the subinterface and enters the subinterface configuration mode.

Step 4	**`encapsulation dot1q`** *`vlan-id`*
	or
	`encapsulation dot1q` *`vlan-id`* **`second-dot1q`** *`inner vlan-id`*
	Example:
	`Router(config-subif)#encapsulation dot1q 100`
	or
	`Router(config-subif)#encapsulation dot1q 100 second-dot1q 1101`
		Defines the encapsulation format as IEEE 802.1Q (dot1q), and specifies the VLAN identifier.
		For double tagging, use the **second-dot1q** keyword and the *inner vlan-id* argument to specify the VLAN tag.

Step 5	**`ethernet loopback permit external`**
	Example:
	`Router(config-subif)#ethernet loopback permit external`
		Configures Ethernet external loopback on the subinterface.

Step 6	**`end`**
	Example:
	`Router(config-subif)#end`
		Exits the subinterface configuration mode.

To start Ethernet data plane loopback, run the following command:

	Command	Purpose
Step 1	**ethernet loopback start local interface gigabitethernet** *slot/port.sub-port* **external timeout** *none* **Example:** `Router#ethernet loopback start local interface gigabitethernet 0/2.1101 external timeout none`	Starts Ethernet external loopback on a subinterface. Enter timeout as *none* to have no time out period for the loopback.

To stop Ethernet data plane loopback, perform the following steps:

	Command	Purpose
Step 1	**ethernet loopback stop local interface gigabitethernet** *slot/port.sub-port* **id** *session-id* **Example:** `Router#ethernet loopback stop local interface gigabitethernet 0/2.1101 id 1`	Stops Ethernet external loopback on a subinterface. Enter the value of the loopback session ID to specify the loopback session that you want to stop.
Step 2	**show ethernet loopback active** **Example:** `Router#show ethernet loopback active`	Displays information to verify if the loopback session has ended.

Configuration Examples for Ethernet Data Plane Loopback

This example shows how to configure Ethernet data plane loopback using single tagging:

```
Router>enable
Router#configure terminal
Router(config)#interface gigabitethernet 0/2.1101
Router(config-subif)#encapsulation dot1q 100
Router(config-subif)#ethernet loopback permit external
Router(config-subif)#end
```

This example shows how to configure Ethernet data plane loopback using double tagging:

```
Router>enable
Router#configure terminal
Router(config)#interface gigabitethernet 0/2.1101
Router(config-subif)#encapsulation dot1q 100 second-dot1q 1101
Router(config-subif)#ethernet loopback permit external
Router(config-subif)#end
```

This example shows how to start an Ethernet data plane loopback:

```
Router#ethernet loopback start local interface gigabitethernet 0/2.1101 external timeout
none
```

```
This is an intrusive loopback and the packets matched with the service will not be able to
pass through. Continue? (yes/[no]):
```

Enter `yes` to continue.

This example shows how to stop an Ethernet data plane loopback:

```
Router#ethernet loopback stop local interface gigabitethernet 0/2.1101 id 1
Router#*Oct 21 10:16:17.887: %E_DLB-6-DATAPLANE_LOOPBACK_STOP: Ethernet Dataplane Loopback
Stop on interface GigabitEthernet0/2 with session id 1
Router#show ethernet loopback active
Total Active Session(s): 0
Total Internal Session(s): 0
Total External Session(s): 0
```

Verifying the Ethernet Data Plane Loopback Configuration

Use the following commands to verify the Ethernet data plane loopback configuration:

- **show ethernet loopback permitted**
- **show ethernet loopback active**

Use the **show ethernet loopback permitted** command to view the loopback capabilities per interface:

```
Router#show ethernet loopback permitted
--------------------------------------------------------------------------------
Interface                              SrvcInst Direction
Dot1q/Dot1ad(s)                        Second-Dot1q(s)
--------------------------------------------------------------------------------
Gi0/2.1101                             N/A      External
100                                    1101
```

Use the **show ethernet loopback active** command to display the summary of the active loopback sessions on a subinterface:

```
Router#show ethernet loopback active
Loopback Session ID      : 1
Interface                : GigabitEthernet0/2.1101
Service Instance         : N/A
Direction                : External
Time out(sec)            : none
Status                   : on
Start time               : *10:17:46.930 UTC Mon Oct 21 2013
Time left                : N/A
Dot1q/Dot1ad(s)          : 100
Second-dot1q(s)          : 1101
Source Mac Address       : Any
Destination Mac Address  : Any
Ether Type               : Any
Class of service         : Any
Llc-oui                  : Any


Total Active Session(s): 1
Total Internal Session(s): 0
Total External Session(s): 1
```

Use the **show ethernet loopback active** command to display the summary of the active loopback sessions on the main interface:

```
Router#show ethernet loopback permitted
Loopback Session ID      : 1
Interface                : GigabitEthernet0/2
```

```
Service Instance        : N/A
Direction               : External
Time out(sec)           : none
Status                  : on
Start time              : *10:14:23.507 UTC Mon Oct 21 2013
Time left               : N/A
Dot1q/Dot1ad(s)         : 1-100
Second-dot1q(s)         : 1-1101
Source Mac Address      : Any
Destination Mac Address : Any
Ether Type              : Any
Class of service        : Any
Llc-oui                 : Any


Total Active Session(s): 1
Total Internal Session(s): 0
Total External Session(s): 1
```

Troubleshooting the Ethernet Data Plane Loopback Configuration

Table 4-2 lists the debug commands to troubleshoot issues pertaining to the Ethernet Data Plane Loopback feature. The Cisco IOS Master Command List at

http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html provides more information about these commands.

Caution Because debugging output is assigned high priority in the CPU process, it can diminish the performance of the router or even render it unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff.

Note Before you run any of the debug commands listed in the following table, ensure that you run the **logging buffered debugging** command, and then turn off console debug logging using the **no logging console** command.

Table 4-2 debug Commands for Ethernet Data Plane Loopback Configuration

debug Command	Purpose
debug elb-pal-pd all	Displays all the debugging information about the Ethernet data plane loopback configuration.
debug elb-pal-pd error	Displays debugging information about Ethernet data plane loopback configuration errors.
debug elb-pal-pd event	Displays debugging information about Ethernet data plane loopback configuration changes.

CFM Support on Routed Port and Port MEP

IEEE Connectivity Fault Management (CFM) is an end-to-end per-service Ethernet-layer Operations, Administration, and Maintenance (OAM) protocol. CFM includes proactive connectivity monitoring, fault verification, and fault isolation for large Ethernet metropolitan-area networks (MANs) and WANs.

Note This feature is supported only if you have purchased the *advipservices* licensing module. For more information about managing software activation licenses on the Cisco ISR and Cisco ISR G2 platforms, see http://www.cisco.com/en/US/docs/routers/access/sw_activation/SA_on_ISR.html.

Restrictions for Configuring Ethernet CFM

- A specific domain must be configured. If it is not, an error message is displayed.
- Multiple domains (different domain names) having the same maintenance level can be configured. However, associating a single domain name with multiple maintenance levels is not permitted.

Configuring Ethernet CFM (Port MEP)

Complete these steps to configure and enable Ethernet CFM on a port Maintenance End Point (MEP):

SUMMARY STEPS

Step 1 **enable**

Step 2 **configure terminal**

Step 3 **ethernet cfm ieee**

Step 4 **ethernet cfm global**

Step 5 **ethernet cfm domain** *domain-name* **level** *value*

Step 6 **service** *service-name* **port**

Step 7 **continuity-check interval** *value*

Step 8 **end**

Step 9 **configure terminal**

Step 10 **interface gigabitethernet** *slot/port*

Step 11 **ethernet cfm mep domain** *domain-name* **mpid** *mpid-value* **service** *service-name*

Step 12 **end**

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `Router>enable`	Enables the privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router#configure terminal`	Enters the global configuration mode.
Step 3	**ethernet cfm ieee** **Example:** `Router(config)#ethernet cfm ieee`	Enables the IEEE version of CFM.
Step 4	**ethernet cfm global** **Example:** `Router(config)#ethernet cfm global`	Enables CFM processing globally on the router.
Step 5	**ethernet cfm domain** *domain-name* **level** *value* **Example:** `Router(config-ecfm)#ethernet cfm domain carrier level 2`	Defines a CFM maintenance domain at a specified level, and enters the Ethernet CFM configuration mode. **level** can be any value from 0 to 7.
Step 6	**service** *service-name* **port** **Example:** `Router(config-ecfm)#service carrier port`	Creates a service on the interface and sets the *config-ecfm-srv* submode.
Step 7	**continuity-check interval** *value* **Example:** `Router(config-ecfm-srv)#continuity-check interval 100m`	Enables sending continuity check messages at the set interval.

Step 8	**end**
	Example:
	`Router(config-ecfm-srv)#end`
		Returns the router to the privileged EXEC mode.

Step 9	**configure terminal** **Example:** `Router#configure terminal`	Enters the global configuration mode.

	Command	Purpose
Step 10	**interface gigabitethernet** *slot/port* **Example:** `Router(config)#interface gigabitethernet 0/2`	Specifies an interface and enters the interface configuration mode.
Step 11	**ethernet cfm mep domain** *domain-name* **mpid** *mpid-value* **service** *service-name* **Example:** `Router(config-if)#ethernet cfm mep domain carrier mpid 44 service carrier`	Sets a port to a maintenance domain and defines it as an MEP. **Note** The values for **domain** and **service** must be the same as the values configured for CFM.

Step 12	**end**
	Example:
	`Router(config-if-ecfm-mep)#end`
		Returns the router to the privileged EXEC mode.

Configuration Example for Ethernet CFM (Port MEP)

This example shows how to configure Ethernet CFM on a port MEP:

```
Router>enable
Router#configure terminal
Router(config)#ethernet cfm ieee
Router(config)#ethernet cfm global
Router(config-ecfm)#ethernet cfm domain carrier level 2
Router(config-ecfm)#service carrier port
Router(config-ecfm-srv)#continuity-check interval 100m
Router(config-ecfm-srv)#end
Router#configure terminal
Router(config)#interface gigabitethernet 0/2
Router(config-if)#ethernet cfm mep domain carrier mpid 44 service carrier
Router(config-if-ecfm-mep)#end
```

Verifying the Ethernet CFM Configuration on a Port MEP

Use the following commands to verify Ethernet CFM configured on a port MEP:

- **show ethernet cfm domain**
- **show ethernet cfm maintenance-points local**
- **show ethernet cfm maintenance-points remote**
- **ping ethernet mpid** *mpid-value* **domain** *domain-name* **service** *service-name* **cos** *value*
- **traceroute ethernet mpid** *mpid-value* **domain** *domain-name* **service** *service-name*
- **show ethernet cfm error configuration**

Use the **show ethernet cfm domain** command to view details about CFM maintenance domains:

```
Router#show ethernet cfm domain carrier
Domain Name: carrier
Level: 2
Total Services: 1
```

```
  Services:
  Type Id   Dir CC CC-int Static-rmep Crosscheck MaxMEP Source  MA-Name
  Port none Dwn Y  100ms  Disabled    Disabled   100    Static  carrier
Router#
```

Use the **show ethernet cfm maintenance-points local** command to view the MEPs that are configured locally on a router. The following is a sample output of the **show ethernet cfm maintenance-points local** command:

```
Router#show ethernet cfm maintenance-points local
Local MEPs:
--------------------------------------------------------------------------------
MPID Domain Name                                 Lvl   MacAddress     Type  CC
Ofld Domain Id                                   Dir   Port           Id
     MA Name                                           SrvcInst       Source
     EVC name
--------------------------------------------------------------------------------
44   carrier                                     2     5657.a844.04fa Port  Y
No   carrier                                     Down  Gi0/2          none
     carrier                                           N/A            Static
     N/A


Total Local MEPs: 1

Local MIPs: None
```

Use the **show ethernet cfm maintenance-points remote** command to display information about remote maintenance point domains or levels. In the following example, carrier, Provider, and customer are the maintenance point domains that are configured:

On router 1:

```
Router1#show ethernet cfm maintenance-points remote
--------------------------------------------------------------------------------
MPID  Domain Name                                 MacAddress          IfSt  PtSt
 Lvl  Domain ID                                   Ingress
 RDI  MA Name                                     Type Id             SrvcInst
      EVC Name                                                        Age
      Local MEP Info
--------------------------------------------------------------------------------
43    carrier                                     5657.a86c.fa92      Up    N/A
 2    carrier                                     Gi0/2
 -    carrier                                     Port none           N/A
      N/A                                                             0s
      MPID: 44 Domain: carrier MA: carrier
33    Provider                                    5657.a86c.fa92      Up    Up
 5    Provider                                    Gi0/2.100
 -    Provider                                    Vlan 100            N/A
      N/A                                                             0s
      MPID: 34 Domain: Provider MA: Provider
3101  customer                                    5657.a86c.fa92      Up    Up
 7    customer                                    Gi0/2.1101
 -    customer1101                                S,C  100,1101       N/A
      N/A                                                             0s
      MPID: 4101 Domain: customer MA: customer1101
3102  customer                                    5657.a86c.fa92      Up    Up
 7    customer                                    Gi0/2.1102
 -    customer1102                                S,C  100,1102       N/A
      N/A                                                             0s
      MPID: 4102 Domain: customer MA: customer1102
```

```
Total Remote MEPs: 4
```

Use the **show ethernet cfm maintenance-points remote** command to view the details of a remote maintenance point domain:

On router 1:

```
Router1#show ethernet cfm maintenance-points remote domain carrier service carrier
--------------------------------------------------------------------------------
MPID  Domain Name                               MacAddress          IfSt  PtSt
 Lvl  Domain ID                                 Ingress
 RDI  MA Name                                   Type Id             SrvcInst
      EVC Name                                                      Age
      Local MEP Info
--------------------------------------------------------------------------------
43    carrier                                   5657.a86c.fa92      Up    Up
 2    carrier                                   Gi0/2
 -    carrier                                   S,C  100,1101       N/A
      N/A                                                           0s
      MPID: 44 Domain: carrier MA: carrier
Total Remote MEPs: 1
```

On router 2:

```
Router2#show ethernet cfm maintenance-points remote domain carrier service carrier
--------------------------------------------------------------------------------
MPID  Domain Name                               MacAddress          IfSt  PtSt
 Lvl  Domain ID                                 Ingress
 RDI  MA Name                                   Type Id             SrvcInst
      EVC Name                                                      Age
      Local MEP Info
--------------------------------------------------------------------------------
44    carrier                                   5657.g945.04fa      Up    Up
 2    carrier                                   Gi0/2
 -    carrier                                   S,C  100,1101       N/A
      N/A                                                           0s
      MPID: 43 Domain: carrier MA: carrier
```

Use the **ping** command to verify if Loopback Messages (LBM) and Loopback Replies (LBR) are successfully sent and received between the routers:

```
Router1#ping ethernet mpid 44 domain carrier service carrier cos 5
Type escape sequence to abort.
Sending 5 Ethernet CFM loopback messages to 5657.a86c.fa92, timeout is 5 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Router1#
```

Use the **traceroute** command to send the Ethernet CFM traceroute messages:

```
Router#traceroute ethernet mpid 44 domain carrier service carrier
Type escape sequence to abort. TTL 64. Linktrace Timeout is 5 seconds
Tracing the route to 5657.a86c.fa92 on Domain carrier, Level 2, service carrier
Traceroute sent via Gi0/2

B = Intermediary Bridge
! = Target Destination
* = Per hop Timeout
--------------------------------------------------------------------------------
                            MAC      Ingress        Ingr Action  Relay Action
  Hops   Host            Forwarded   Egress         Egr Action   Previous Hop
--------------------------------------------------------------------------------
```

```
! 1                    5657.a86c.fa92 Gi0/2          IngOk        RlyHit:MEP
                       Not Forwarded                              5657.g945.04fa
Router#
```

Configuring Ethernet CFM (Single-Tagged Packets)

Complete these steps to configure and enable Ethernet CFM for single-tagged packets:

SUMMARY STEPS

Step 1 **enable**

Step 2 **configure terminal**

Step 3 **ethernet cfm ieee**

Step 4 **ethernet cfm global**

Step 5 **ethernet cfm domain** *domain-name* **level** *level-id*

Step 6 **service** *service-name* **vlan** *vlan-id* **direction down**

Step 7 **continuity-check**

Step 8 **interface gigabitethernet** *slot/port*

Step 9 **ethernet cfm mep domain** *domain-name* **mpid** *value* **service** *service-name*

Step 10 **interface gigabitethernet** *slot/port.subinterface*

Step 11 **encapsulation dot1q** *vlan-id*

Step 12 **end**

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `Router>enable`	Enables the privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router#configure terminal`	Enters the global configuration mode.
Step 3	**ethernet cfm ieee** **Example:** `Router(config)#ethernet cfm ieee`	Enables the IEEE version of CFM.
Step 4	**ethernet cfm global** **Example:** `Router(config)#ethernet cfm global`	Enables CFM processing globally on the router.

	Command	Purpose
Step 5	**ethernet cfm domain** *domain-name* **level** *value* **Example:** `Router(config)#ethernet cfm domain customer level 7`	Defines a CFM maintenance domain at a specified level, and enters the Ethernet CFM configuration mode. **level** can be any value from 0 to 7.
Step 6	**service** *service-name* **vlan** *vlan-id* **direction down** **Example:** `Router(config-ecfm)#service customer1101 vlan 100 direction down`	Enters the CFM service configuration mode. **vlan**—Specifies the VLAN.
Step 7	**continuity-check** **Example:** `Router(config-ecfm-srv)#continuity-check`	Enables sending continuity check messages.
Step 8	**interface gigabitethernet** *slot/port* **Example:** `Router(config-ecfm-srv)#interface gigabitethernet 0/2`	Specifies an interface and enters the interface configuration mode.
Step 9	**ethernet cfm mep domain** *domain-name* **mpid** *mpid-value* **service** *service-name* **Example:** `Router(config-if)#ethernet cfm mep domain customer mpid 100 service customer1101`	Sets a port to a maintenance domain and defines it as an MEP. **Note** The values for **domain** and **service** must be the same as the values that were configured for CFM.
Step 10	**interface gigabitethernet** *slot/port.subinterface* **Example:** `Router(config-if-ecfm-mep)#interface gigabitethernet 0/2.1`	Specifies a subinterface and enters the subinterface configuration mode.
Step 11	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-subif)#encapsulation dot1q 100`	Defines the encapsulation format as IEEE 802.1Q (dot1q), and specifies the VLAN identifier.

Step 12	**end**
	Example:
	`Router(config-subif)#end`
		Returns the router to the privileged EXEC mode.

Configuration Example for Ethernet CFM (Single-Tagged Packets)

This example shows how to configure Ethernet CFM for single-tagged packets:

```
Router>enable
Router#configure terminal
Router(config)#ethernet cfm ieee
Router(config)#ethernet cfm global
Router(config)#ethernet cfm domain customer level 7
Router(config-ecfm)#service customer1101 vlan 100 direction down
Router(config-ecfm-srv)#continuity-check
Router(config)#interface gigabitethernet 0/2
Router(config-if)#ethernet cfm mep domain customer mpid 100 service customer1101
Router(config-if-ecfm-mep)#interface gigabitethernet 0/2.1
Router(config-subif)#encapsulation dot1q 100
Router(config-subif)#end
```

Verifying the Ethernet CFM Configuration for Single-Tagged Packets

Use the following commands to verify Ethernet CFM configured for single-tagged packets:

- **show ethernet cfm domain**
- **show ethernet cfm maintenance-points local**
- **show ethernet cfm maintenance-points remote**
- **show ethernet cfm error configuration**

Use the **show ethernet cfm domain** command to display the maintenance point domains configured in the network. In the following example, the customer, enterprise, and carrier maintenance point domains are configured.

```
Router#show ethernet cfm domain
Domain Name: customer
Level: 7
Total Services: 1
  Services:
  Type Id   Dir CC CC-int Static-rmep Crosscheck MaxMEP Source  MA-Name
  Vlan 100  Dwn Y  10s    Disabled    Disabled   100    Static  customer1101

Domain Name: enterprise
Level: 6
Total Services: 1
  Services:
  Type Id   Dir CC CC-int Static-rmep Crosscheck MaxMEP Source  MA-Name
  Vlan 110  Dwn Y  10s    Disabled    Disabled   100    Static  custservice

Domain Name: carrier
Level: 2
Total Services: 1
  Services:
  Type Id   Dir CC CC-int Static-rmep Crosscheck MaxMEP Source  MA-Name
  Vlan 200  Dwn Y  10s    Disabled    Disabled   100    Static  carrier
Router#
```

Use the **show ethernet cfm maintenance-points local** command to view the local MEPs. The following is a sample output of the **show ethernet cfm maintenance-points local** command:

```
Router#show ethernet cfm maintenance-points local
--------------------------------------------------------------------------------
MPID Domain Name                                Lvl   MacAddress     Type  CC
Ofld Domain Id                                  Dir   Port           Id
```

```
     MA Name                                           SrvcInst       Source
     EVC name
--------------------------------------------------------------------------------
100  customer                                    7     70ca.9b4d.a400 Vlan  Y
No   customer                                    Down  Gi0/2          100
     customer1101                                      N/A            Static
     N/A
400  enterprise                                  6     70ca.9b4d.a400 Vlan  I
No   enterprise                                  Down  Gi0/1          110
     custservice                                       N/A            Static
     N/A
44   carrier                                     2     70ca.9b4d.a400 Vlan  N
No   carrier                                     Down  Gi0/2          200
     carrier                                           N/A            Static
     N/A

Total Local MEPs: 3

Local MIPs: None
Router#
```

Use the **show ethernet cfm maintenance-points remote** command to display information about remote maintenance point domains or levels.

The following example displays the continuity check messages exchanged between remote MEPs:

On router 1:

```
Router1#show ethernet cfm maintenance-points remote
-----------------------------------------------------------------------------------------
MPID Domain Name             MacAddress           IfSt               PtSt
 Lvl Domain                  Ingress
 RDI MA                      Type Id              SrvcInst
     EVC Name                                     Age
     Local MEP Info
-----------------------------------------------------------------------------------------
110  customer                70ca.9b4d.a400       Up                  Up
 7   customer                Gi0/2
 -   customer1101            Vlan 100             N/A
     N/A                                          12s
     MPID: 100 Domain: customer MA: customer1101

410  enterprise              70ca.9b4d.a400       Up                  Up
 6   enterprise              Gi0/1
 -   custservice             Vlan 110             N/A
     N/A                                          12s
     MPID: 400 Domain: enterprise MA: custservice

43   carrier                 70ca.9b4d.a400       Up                  Up
 2   carrier                 Gi0/2
 -   carrier                 Vlan 200             N/A
     N/A                                          12s
     MPID: 44  Domain: carrier MA: carrier

Total Remote MEPs: 3
Router1#
```

On router 2:

```
Router2#show ethernet cfm maintenance-points remote
-----------------------------------------------------------------------------------------
MPID Domain Name             MacAddress           IfSt               PtSt
 Lvl Domain                  Ingress
 RDI MA                      Type Id              SrvcInst
     EVC Name                                     Age
     Local MEP Info
-----------------------------------------------------------------------------------------
100  customer                0026.99f7.0b41       Up                  Up
 7   customer                Gi0/2
 -   customer1101            Vlan 100             N/A
     N/A                                          2s
     MPID: 110 Domain: customer MA: customer1101

400  enterprise              0026.99f7.0b41       Up                  Up
 6   enterprise              Gi0/1
 -   custservice             Vlan 110             N/A
     N/A                                          2s
     MPID: 410 Domain: enterprise MA: custservice

44   carrier                 0026.99f7.0b41       Up                  Up
 2   carrier                 Gi0/2
 -   carrier                 Vlan 200             N/A
     N/A                                          2s
     MPID: 43  Domain: carrier MA: carrier

Total Remote MEPs: 3
Router2#
```

Use the **show ethernet cfm error configuration** command to view Ethernet CFM configuration errors (if any). The following is a sample output of the **show ethernet cfm error configuration** command:

```
Router#show ethernet cfm error configuration
--------------------------------------------------------------------------------
CFM Interface      Type  Id       Level    Error type
--------------------------------------------------------------------------------
Gi0/2              S,C   100      5        CFMLeak
```

Configuring Ethernet CFM (Double-Tagged Packets)

Complete these steps to configure and enable Ethernet CFM for double-tagged packets:

SUMMARY STEPS

Step 1 **enable**

Step 2 **configure terminal**

Step 3 **ethernet cfm ieee**

Step 4 **ethernet cfm global**

Step 5 **ethernet cfm domain** *domain-name* **level** *value*

Step 6 **service** *service-name* **vlan** *vlan-id* **inner-vlan** *inner-vlan-id* **direction down**

Step 7 **continuity-check**

Step 8 **interface gigabitethernet** *slot/port*

Step 9 **ethernet cfm mep domain** *domain-name* **mpid** *mpid-value* **service** *service-name*

Step 10 **interface gigabitethernet** *slot/port.subinterface*

Step 11 **encapsulation dot1q** *vlan-id* **second-dot1q** *inner vlan-id*

Step 12 **end**

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `Router>enable`	Enables the privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router#configure terminal`	Enters the global configuration mode.
Step 3	**ethernet cfm ieee** **Example:** `Router(config)#ethernet cfm ieee`	Enables the IEEE version of CFM.
Step 4	**ethernet cfm global** **Example:** `Router(config)#ethernet cfm global`	Enables CFM processing globally on the router.
Step 5	**ethernet cfm domain** *domain-name* **level** *0 to 7* **Example:** `Router(config-ecfm)#ethernet cfm domain customer level 7`	Defines a CFM maintenance domain at a specified level, and enters Ethernet CFM configuration mode. **level** can be any value from 0 to 7.
Step 6	**service** *service-name* **vlan** *vlan-id* **inner-vlan** *inner vlan-id* **direction down** **Example:** `Router(config-ecfm)#service customer1101 vlan 100 inner-vlan 30 direction down`	Enters the CFM service configuration mode. The following are the parameters: • **vlan**—Specifies the VLAN. • **inner-vlan**—The **inner-vlan** keyword and the *inner vlan-id* argument specify the VLAN tag for double-tagged packets.
Step 7	**continuity-check** **Example:** `Router(config-ecfm-srv)#continuity-check`	Enables sending continuity check messages.
Step 8	**interface gigabitethernet** *slot/port* **Example:** `Router(config-ecfm-srv)#interface gigabitethernet 0/2`	Specifies an interface and enters the interface configuration mode.

	Command	Purpose

Step 9	`ethernet cfm mep domain` *`domain-name`* `mpid` *`mpid-value`* `service` *`service-name`*
	Example:
	`Router(config-if)#ethernet cfm mep domain customer mpid 100 service customer1101`
		Sets a port to a maintenance domain and defines it as an MEP.
		Note The values for **domain** and **service** must be the same as the values configured for CFM.
		MPID—Specifies the maintenance endpoint identifier.

Step 10	`interface gigabitethernet` *`slot/port.subinterface`*
	Example:
	`Router(config-if-ecfm-mep)#interface gigabitethernet 0/2.1101`
		Specifies a subinterface and enters the subinterface configuration mode.

Step 11	`encapsulation dot1q` *`vlan-id`* `second-dot1q` *`inner vlan-id`*
	Example:
	`Router(config-subif)#encapsulation dot1q 100 second-dot1q 30`
		Defines the encapsulation format as IEEE 802.1Q (dot1q), and specifies the VLAN identifier.
		Use the **second-dot1q** keyword and the *inner vlan-id* argument to specify the VLAN tag.

Step 12	`end`
	Example:
	`Router(config-subif)#end`
		Returns the router to the privileged EXEC mode.

Configuration Example for Ethernet CFM (Double-Tagged Packets)

This example shows how to configure Ethernet CFM for double-tagged packets:

```
Router>enable
Router#configure terminal
Router(config)#ethernet cfm ieee
Router(config)#ethernet cfm global
Router(config-ecfm)#ethernet cfm domain customer level 7
Router(config-ecfm)#service customer1101 vlan 100 inner-vlan 30 direction down
Router(config-ecfm-srv)#continuity-check
Router(config-ecfm-srv)#interface gigabitethernet 0/2
Router(config-if)#ethernet cfm mep domain customer mpid 100 service customer1101
Router(config-if-ecfm-mep)#interface gigabitethernet 0/2.1101
Router(config-subif)#encapsulation dot1q 100 second-dot1q 30
Router(config-subif)#end
```

Verifiying the Ethernet CFM Configuration for Double-Tagged Packets

Use the following commands to verify Ethernet CFM configured for double-tagged packets:

- **show ethernet cfm maintenance-points local**
- **show ethernet cfm maintenance-points remote**
- **ping ethernet mpid** *mpid-value* **domain** *domain-name* **service** *service-name* **cos** *value*
- **traceroute ethernet mpid** *mpid-value* **domain** *domain-name* **service** *service-name*
- **show ethernet cfm error configuration**

Use the **show ethernet cfm maintenance-points local** command to view the local MEPs. The following is a sample output of the **show ethernet cfm maintenance-points local** command:

```
Router#show ethernet cfm maintenance-points local
----------------------------------------------------------------------------------
MPID Domain Name          MacAddress                 IfSt                   PtSt
 Lvl Domain ID          Ingress
 RDI MA Name              Type Id                    SrvcInst
     EVC Name                              Age
     Local MEP Info
----------------------------------------------------------------------------------
100  customer             8843.e154.6f01             Up                     Up
 7   customer             Gi0/2.1101
 -   customer1101         S, C 100, 30               N/A
     N/A                                   58s
     MPID: 100 Domain: customer MA: customer1101
Router#
```

Use the **show ethernet cfm maintenance-points remote** command to display the remote maintenance point domains. In the following example, customer, carrier, and enterprise are the maintenance point domains that are configured:

On router 1:

```
Router1#show ethernet cfm maintenance-points remote
----------------------------------------------------------------------------------
MPID Domain Name          MacAddress                 IfSt                   PtSt
 Lvl Domain ID          Ingress
 RDI MA Name              Type Id                    SrvcInst
     EVC Name                                        Age
     Local MEP Info
----------------------------------------------------------------------------------
110  customer             8843.e154.6f01             Up                     Up
 7   customer             Gi0/2.1101
 -   customer1101         S, C 100, 30               N/A
     N/A                                             58s
     MPID: 100 Domain: customer MA: customer1101

43   carrier             8843.e154.6f01              Up                     Up
 2   carrier             Gi0/2.2
 -   carrier             S, C 50, 20                 N/A
     N/A                                             58s
     MPID: 44 Domain: carrier MA: carrier

410  enterprise          8843.e154.6f01              Up                     Up
 6   enterprise          Gi0/1.1
 -   custservice         S, C 200, 70                N/A
     N/A                                             58s
     MPID: 400 Domain: enterprise MA: custservice

Router1#
```

On router 2:

```
Router2#show ethernet cfm maintenance-points remote
----------------------------------------------------------------------------------
MPID Domain Name          MacAddress                 IfSt                   PtSt
 Lvl Domain ID          Ingress
 RDI MA Name              Type Id                    SrvcInst
     EVC Name                                        Age
     Local MEP Info
----------------------------------------------------------------------------------
```

```
100  customer             0026.99f7.0b41             Up                     Up
 7   customer             Gi0/2.1101
 -   customer1101         S, C 100, 30               N/A
     N/A                                             40s
     MPID: 110 Domain: customer MA: customer1101

44   carrier             0026.99f7.0b41              Up                     Up
 2   carrier             Gi0/2.2
 -   carrier             S, C 50, 20                 N/A
     N/A                                             40s
     MPID: 43 Domain: carrier MA: carrier

400  enterprise          0026.99f7.0b41              Up                     Up
 6   enterprise          Gi0/1.1
 -   custservice         S, C 200, 70                N/A
     N/A                                             40s
     MPID: 410 Domain: enterprise MA: custservice

Router2#
```

Use the **ping** command to verify if Ethernet CFM loopback messages are successfully sent and received between the routers:

```
Router#ping ethernet mpid 100 domain customer service customer1101  cos 5
Type escape sequence to abort.
Sending 5 Ethernet CFM loopback messages to 8843.e154.6f01, timeout is 5 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Router#
```

Use the **traceroute** command to send the Ethernet CFM traceroute messages:

```
Router#traceroute ethernet mpid 100 domain customer service customer1101
Type escape sequence to abort. TTL 64. Linktrace Timeout is 5 seconds
Tracing the route to 8843.e154.6f01 on Domain customer, Level 7, service customer1101,
vlan 100 inner-vlan 30
Traceroute sent via Gi0/2.1101

B = Intermediary Bridge
! = Target Destination
* = Per hop Timeout
--------------------------------------------------------------------------------
                             MAC      Ingress        Ingr Action  Relay Action
  Hops   Host             Forwarded   Egress         Egr Action   Previous Hop
--------------------------------------------------------------------------------
! 1                    8843.e154.6f01 Gi0/2.1101 IngOk        RlyHit:MEP
                       Not Forwarded                              5657.a86c.fa92
```

Use the **show ethernet cfm error configuration** command to view Ethernet CFM configuration errors (if any). The following is a sample output of the **show ethernet cfm error configuration** command:

```
Router#show ethernet cfm error configuration
--------------------------------------------------------------------------------
CFM Interface      Type  Id         Level    Error type
--------------------------------------------------------------------------------
Gi0/2              S,C   100,30     5        CFMLeak
Gi0/2              S,C   100,30     1        CFMLeak
```

Troubleshooting Ethernet CFM Configuration

Table 4-3 lists the debug commands to troubleshoot issues pertaining to the Ethernet CFM configuration.

The Cisco IOS Master Command List at

http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html provides more information about these commands.

Caution Because debugging output is assigned high priority in the CPU process, it can diminish the performance of the router or even render it unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff.

Note Before you run any of the debug commands listed in the following table, ensure that you run the **logging buffered debugging** command, and then turn off console debug logging using the **no logging console** command.

Table 4-3 debug Commands for Ethernet CFM Configuration

debug Command	Purpose
debug ethernet cfm all	Enables all Ethernet CFM debug messages.
debug ethernet cfm diagnostic	Enables low-level diagnostic debugging of Ethernet CFM general events or packet-related events.
debug ethernet cfm error	Enables debugging of Ethernet CFM errors.
debug ethernet cfm packets	Enables debugging of Ethernet CFM message packets.
debug ecfmpal all	Enables debug messages for all Ethernet CFM platform events.
debug ecfmpal api	Displays debug messages for all Ethernet CFM platform API events.
debug ecfmpal common	Displays debug messages for all Ethernet CFM platform common events.
debug ecfmpal ecfmpal	Enables debugging of all Ethernet CFM platform events.
debug ecfmpal epl	Enables debugging of all Ethernet CFM platform endpoint list (EPL) events.
debug ecfmpal isr	Enables debugging of all Ethernet CFM platform interrupt service request (ISR) events.

Support for Y.1731 Performance Monitoring on Routed Port (L3 Subinterface)

Y.1731 Performance Monitoring (PM) provides a standard Ethernet PM function that includes measurement of Ethernet frame delay, frame delay variation, frame loss, and frame throughput measurements specified by the ITU-T Y-1731 standard and interpreted by the Metro Ethernet Forum (MEF) standards group.

Note This feature is supported only if you have purchased the *advipservices* licensing module. For more information about managing software activation licenses on the Cisco ISR and Cisco ISR G2 platforms, see http://www.cisco.com/en/US/docs/routers/access/sw_activation/SA_on_ISR.html.

Frame Delay

Ethernet frame delay measurement is used to measure frame delay and frame delay variations. Ethernet frame delay is measured using the Delay Measurement Message (DMM) method.

Restrictions for Configuring Two-Way Delay Measurement

Follow the guidelines and restrictions listed here when you configure two-way delay measurement:

- Y.1731 PM measurement works only for a point-to-point network topology.
- The granularity of the clock for delay measurement is in seconds and nanoseconds.
- CFM Y.1731 packets work with a maximum of two VLAN tags. The expected behavior is not observed with more VLAN tags. Also, CFM Y.1731 packets do not work with untagged cases.

Configuring Two-Way Delay Measurement

The following steps show how to configure two-way delay measurement. Both single and double tagging methods are included in the steps listed below.

SUMMARY STEPS

Step 1	**enable**
Step 2	**configure terminal**
Step 3	**ip sla** *operation number*
Step 4	**ethernet y1731 delay** *DMM* **domain** *value* **vlan** *vlan-id* **mpid** *value* **cos** *value* **source mpid** *value* or **ethernet y1731 delay** *DMM* **domain** *value* **vlan** *vlan-id* **inner-vlan** *inner vlan-id* **mpid** *value* **cos** *value* **source mpid** *value*
Step 5	**aggregate interval** *seconds*
Step 6	**exit**
Step 7	**ip sla schedule** *operation number* **start-time** {*start time* | *now*}
Step 8	**end**

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**ip sla** *operation number* **Example:** `Router(config)# ip sla 1101`	Enables the IP SLA configuration. *operation-number*—The IP SLA operation you want to configure.

Step 4	**ethernet y1731 delay** *DMM* **domain** *value* **vlan** *vlan-id* **mpid** *value* **cos** *value* **source mpid** *value*
	or
	ethernet y1731 delay *DMM* **domain** *value* **vlan** *vlan-id* **inner-vlan** *inner vlan-id* **mpid** *value* **cos** *value* **source mpid** *value*
	Example:
	`Router(config-ip-sla)# ethernet y1731 delay DMM domain customer vlan 100 mpid 3101 cos 1 source mpid 4101`
	or
	`Router(config-ip-sla)# ethernet y1731 delay DMM domain customer vlan 100 inner-vlan 1101 mpid 3101 cos 1 source mpid 4101`
		Configures a two-way delay measurement.
		Note Both single tagging and double tagging are supported.
		The following are the parameters:
		• **delay**—Specifies the delay distribution parameter.
		Note DMM is the only supported delay distribution parameter.
		• **vlan**—Specifies the VLAN.
		• **inner-vlan**—The **inner-vlan** keyword and the *inner vlan-id* argument specify the VLAN tag for double-tagged packets.
		• **cos**—Specifies the CoS. The value can be any number between 0 and 7.
		Note For double-tagged packets, the **cos** value corresponds to the value specified for the outer tag.
		• **mpid**—Specifies the destination MPID.
		• **source**—Specifies the source MPID.

Step 5	**aggregate interval** *seconds* **Example:** `Router(config-sla-y1731-delay)# aggregate interval 30`	Configures the Y.1731 aggregation parameter, where **aggregate interval** refers to the interval at which the packets are sent. *seconds*—Specifies the length of time, in seconds.

	Command	Purpose
Step 6	**exit** **Example:** `Router(config-sla-y1731-delay)# exit`	Exits the router configuration mode.
Step 7	**ip sla schedule** *operation number* **life** {*value* | *forever*} **start-time** *value* **Example:** `Router(config)#ip sla schedule 1101 life forever start-time now`	Schedules the two-way delay measurement. • **life**—Specifies a period of time (in seconds) to execute. The value can also be set as *forever.* • **start-time**—Specifies the time at which to start the entry. The options available are *after, hh:mm, hh:mm:ss, now,* and *pending*.

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

Configuration Examples for Two-Way Delay Measurement

This example shows how to configure two-way delay measurement using single tagging:

```
router>enable
router#configure terminal
router(config)#ip sla 1101
router(config-ip-sla)#ethernet y1731 delay DMM domain customer vlan 100 mpid 3101 cos 1
router(config-sla-y1731-delay)#aggregate interval 30
router(config-sla-y1731-delay)#exit
router(config)#ip sla schedule 1102 life forever start-time now
router(config)#end
```

This example shows how to configure two-way delay measurement using double tagging:

```
router>enable
router#configure terminal
router(config)#ip sla 1101
router(config-ip-sla)#ethernet y1731 delay DMM domain customer vlan 100 inner-vlan 1101
mpid 3101 cos 1 source mpid 4101
router(config-sla-y1731-delay)#aggregate interval 30
router(config-sla-y1731-delay)#exit
router(config)#ip sla schedule 1101 life forever start-time now
router(config)#end
```

Verifying Two-Way Delay Measurement Configuration

Use the following commands to verify the performance-monitoring sessions:

- **show run | sec ip sla**
- **show ip sla summary**
- **show ip sla statistics** *entry-number*
- **show ip sla configuration** *entry-number*
- **show ethernet cfm pm session summary**
- **show ethernet cfm pm session detail** *session-id*

- **show ethernet cfm pm session db** *session-id*

The following are the sample outputs of the commands listed above:

```
Router#show run | sec ip sla
ip sla auto discovery
ip sla 1101
 ethernet y1731 delay DMM domain customer vlan 100 inner-vlan 1101 mpid 3101 cos
 1 source mpid 4101
ip sla schedule 1101 life forever start-time now

Router#show ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending

ID           Type        Destination       Stats       Return      Last
                                           (ms)        Code        Run
-----------------------------------------------------------------------
*1101        y1731-delay Domain:customer V -           OK          27 seconds ag
                         lan:100 CVlan:110                         o
                         1 Mpid:3101

Router#show ip sla statistics
IPSLAs Latest Operation Statistics

IPSLA operation id: 1101
Delay Statistics for Y1731 Operation 1101
Type of operation: Y1731 Delay Measurement
Latest operation start time: *10:43:12.930 UTC Mon Oct 21 2013
Latest operation return code: OK
Distribution Statistics:
Interval
 Start time:  *10:43:12.930 UTC Mon Oct 21 2013
 Elapsed time: 15 seconds
 Number of measurements initiated: 7
 Number of measurements completed: 7
 Flag: OK

Router#show ip sla configuration 1101
IP SLAs Infrastructure Engine-III
Entry number: 1101
Owner:
Tag:
Operation timeout (milliseconds): 5000
Ethernet Y1731 Delay Operation
Frame Type: DMM
Domain: customer
Vlan: 100
CVlan: 1101
Target Mpid: 3101
Source Mpid: 4101
CoS: 1
   Max Delay: 5000
   Request size (Padding portion): 64
   Frame Interval: 1000
   Clock: Not In Sync
Threshold (milliseconds): 5000
Schedule:
   Operation frequency (seconds): 30  (not considered if randomly scheduled)
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): Forever
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Statistics Parameters
  Frame offset: 1
  Distribution Delay Two-Way:
   Number of Bins 10
   Bin Boundaries: 5000,10000,15000,20000,25000,30000,35000,40000,45000,-1
  Distribution Delay-Variation Two-Way:
   Number of Bins 10
   Bin Boundaries: 5000,10000,15000,20000,25000,30000,35000,40000,45000,-1
  Aggregation Period: 30
History
  Number of intervals: 2

Router#show ethernet cfm pm session summary
Number of Configured Session : 150
Number of Active Session: 2
Number of Inactive Session: 148
Router#

Router(config)#show ethernet cfm pm session detail 0
Session ID: 0
Sla Session ID: 1101
Level: 7
Service Type: S,C
Service Id: 100,1101
Direction: Down
Source Mac: 5352.a824.04fr
Destination Mac: 5067.a87c.fa92
Session Version: 0
Session Operation: Proactive
Session Status: Active
MPID: 4101
Tx active: yes
Rx active: yes
RP monitor Tx active: yes
RP monitor Rx active: yes
Timeout timer: stopped
Last clearing of counters: *00:00:00.000 UTC Mon Jan 1 1900
DMMs:
   Transmitted: 117
DMRs:
   Rcvd: 117
1DMs:
   Transmitted: 0
   Rcvd: 0
LMMs:
   Transmitted: 0
LMRs:
   Rcvd: 0
VSMs:
   Transmitted: 0
VSRs:
   Rcvd: 0
SLMs:
   Transmitted: 0
SLRs:
   Rcvd: 0
Test ID 0
Router1#
```

```
Router#show ethernet cfm pm session db 0
----------------------------------------------------------------------------
      TX Time FWD                   RX Time FWD
      TX Time BWD                   RX Time BWD              Frame Delay
      Sec:nSec                      Sec:nSec                  Sec:nSec
----------------------------------------------------------------------------
Session ID: 0
****************************************************************************
3591340722:930326034           3591340663:866791722
3591340663:866898528           3591340722:930707484            0:274644
****************************************************************************
3591340723:927640626           3591340664:864091056
3591340664:864182604           3591340723:927976302            0:244128
****************************************************************************
3591340724:927640626           3591340665:864091056
3591340665:864167346           3591340724:927961044            0:244128
****************************************************************************
3591340725:927671142           3591340666:864121572
3591340666:864213120           3591340725:928006818            0:244128
****************************************************************************
3591340726:927655884           3591340667:864106314
3591340667:864197862           3591340726:927991560            0:244128
****************************************************************************
3591340727:927732174           3591340668:864167346
3591340668:864533538           3591340727:928327236            0:228870
****************************************************************************
3591340728:927655884           3591340669:864121572
3591340669:864197862           3591340728:928006818            0:274644
****************************************************************************
3591340729:927671142           3591340670:864121572
3591340670:864197862           3591340729:927991560            0:244128
****************************************************************************
```

Troubleshooting Two-Way Delay Measurement Configuration

Table 4-4 lists the debug commands to troubleshoot issues pertaining to the two-way delay measurement configuration.

The Cisco IOS Master Command List at

http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html provides more information about these commands.

Caution Because debugging output is assigned high priority in the CPU process, it can diminish the performance of the router or even render it unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff.

Note Before you run any of the debug commands listed in the following table, ensure that you run the **logging buffered debugging** command, and then turn off console debug logging using the **no logging console** command.

Table 4-4 debug Commands for Two-Way Delay Measurement Configuration

debug Command	Purpose
debug epmpal all	Enables debugging of all Ethernet performance monitoring (PM) events.
debug epmpal api	Enables debugging of Ethernet PM API events.
debug epmpal rx	Enables debugging of Ethernet PM packet-receive events.
debug epmpal tx	Enables debugging of Ethernet PM packet-transmit events.

CHAPTER 4

Configuring Power Managment

The following sections provide information about configuring power management and Power-over-Ethernet (PoE) for router models that support these features. See specific router model documentation for information about supported features:

- Monitoring Power Usage with EnergyWise, page 4-1
- Configuring Power-over-Ethernet, page 4-1

Monitoring Power Usage with EnergyWise

Cisco EnergyWise monitors and manages the power usage of network devices and devices connected to the network. For information about using EnergyWise technology, see the configuration guides at the following site:

http://www.cisco.com/en/US/products/ps10195/products_installation_and_configuration_guides_list.html

Configuring Power-over-Ethernet

Use the **power inline** command to enable/disable or the **show power inline** command to verify Power-over-Ethernet (PoE).

Note Power-over-Ethernet is available for the C867VAE-POE-W-A-K9 model, using port FE0, with a 60-W power supply.

- Enabling/Disabling Power-over-Ethernet, page 4-1
- Verifying the Power-over-Ethernet Configuration on the Interface, page 4-2

Enabling/Disabling Power-over-Ethernet

Use the **power inline** command to enable/disable Power-over-Ethernet (PoE) on the Fast Ethernet (FE) port 0. Beginning in privileged EXEC mode, perform these steps.

SUMMARY STEPS

1. **configure terminal**
2. **interface fastethernet 0**
3. **power inline {auto | never}**
4. **end**

DETAILED STEPS

	Command	Purpose
Step 1	`Router#` **`configure terminal`**	Enters global configuration mode.
Step 2	`Router(config)#` **`interface fastethernet 0`**	The Fast Ethernet (FE) 0 interface. **Note** The C867VAE-POE-W-A-K9 supports Power-over-Ethernet on the FE0 interface only.
Step 3	`Router(config-if)#` **`power inline {auto | never}`**	Use **auto** to configure the port to supply inline power automatically. Use **never** to disable inline power on the port.

Step 4	`Router(config-if)#` **`end`**
	`Router#`
		Exits configuration mode.

Verifying the Power-over-Ethernet Configuration on the Interface

Use the **show power inline** command to verify the power configuration on the FE0 port.

```
Router# show power inline
PowerSupply   SlotNum.   Maximum   Allocated       Status
-----------   --------   -------   ---------       ------
INT-PS            0        18.000     6.300         PS GOOD
Interface   Config   Device   Powered    PowerAllocated
---------   ------   ------   -------    --------------
Fa0         auto     Cisco    On         6.300 Watts
```

CHAPTER 5

Configuring Security Features

This chapter provides an overview of authentication, authorization, and accounting (AAA), which is the primary Cisco framework for implementing selected security features that can be configured on the Cisco 860 and Cisco 880 series Integrated Services Routers (ISRs).

This chapter contains the following sections:

Authentication, Authorization, and Accounting

AAA network security services provide the primary framework through which you set up access control on your router. Authentication provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and depending on the security protocol you choose, encryption. Authorization provides the method for remote access control, including one-time authorization or authorization for each service; per-user account list and profile; user group support; and support of IP, Internetwork Packet Exchange (IPX), AppleTalk Remote Access (ARA), and Telnet. Accounting provides the method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.

AAA uses protocols such as RADIUS, TACACS+, or Kerberos to administer its security functions. If your router is acting as a network access server, AAA is the means through which you establish communication between your network access server and your RADIUS, TACACS+, or Kerberos security server.

For information about configuring AAA services and supported security protocols, see the following sections of *Cisco IOS Security Configuration Guide: Securing User Services, Release 12.4T* :

- Configuring Authentication
- Configuring Authorization
- Configuring Accounting
- RADIUS and TACACS+ Attributes
- Configuring Kerberos

Configuring AutoSecure

The AutoSecure feature disables common IP services that can be exploited for network attacks and enables IP services and features that can aid in the defense of a network when under attack. These IP services are all disabled and enabled simultaneously with a single command, which simplifies security configuration on your router. For a complete description of the AutoSecure feature, see *AutoSecure*.

Configuring Access Lists

Access lists permit or deny network traffic over an interface based on source IP address, destination IP address, or protocol. Access lists are configured as standard or extended. A standard access list either permits or denies passage of packets from a designated source. An extended access list allows designation of both the destination and the source, and it allows designation of individual protocols to be permitted or denied passage.

For more complete information on creating access lists, see the "Access Control Lists (ACLs)" section in *Cisco IOS Security Configuration Guide: Securing the Data Plane, Release 12.4T*.

An access list is a series of commands with a common tag to bind them together. The tag is either a number or a name. Table 5-1 lists the commands used to configure access lists.

Table 5-1 Access List Configuration Commands

ACL Type	Configuration Commands
Numbered	
Standard	**access-list** {**1-99**}{**permit** | **deny**} *source-addr* [*source-mask*]
Extended	**access-list** {**100-199**}{**permit** | **deny**} *protocol source-addr* [*source-mask*] *destination-addr* [*destination-mask*]
Named	
Standard	**ip access-list standard** *name* **deny** {*source* | *source-wildcard* | **any**}
Extended	**ip access-list extended** *name* **{permit** | **deny}** *protocol* {*source-addr*[*source-mask*] | **any**}{*destination-addr* [*destination-mask*] | **any**}

To create, refine, and manage access lists, see the "Access Control Lists (ACLs)" section in *Cisco IOS Security Configuration Guide: Securing the Data Plane, Release 12.4T*:

- Creating an IP Access List and Applying It to an Interface
- Creating an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values
- Refining an IP Access List
- Displaying and Clearing IP Access List Data Using ACL Manageability

Access Groups

An access group is a sequence of access list definitions bound together with a common name or number. This group is enabled for an interface during interface configuration. Use the following guidelines when creating access groups.

- The order of access list definitions is significant. A packet is compared against the first access list in the sequence. If there is no match (that is, if neither a permit nor a deny occurs), the packet is compared with the next access list, and so on.
- All parameters must match the access list before the packet is permitted or denied.
- There is an implicit "deny all" at the end of all sequences.

For information on configuring and managing access groups, see *Cisco IOS Security Configuration Guide: Securing the Data Plane, Release 12.4T.*

Configuring Cisco IOS Firewall

The Cisco IOS Firewall lets you configure a stateful firewall in which packets are inspected internally and the state of network connections is monitored. A stateful firewall is superior to static access lists because access lists can only permit or deny traffic based on individual packets, not based on streams of packets. Also, because Cisco IOS Firewall inspects the packets, decisions to permit or deny traffic can be made by examining application layer data, which static access lists cannot examine.

To configure a Cisco IOS Firewall, specify which protocols to examine by using the following command in interface configuration mode:

ip inspect name *inspection-name protocol* **timeout** *seconds*

When inspection detects that the specified protocol is passing through the firewall, a dynamic access list is created to allow the passage of return traffic. The timeout parameter specifies the length of time the dynamic access list remains active without return traffic passing through the router. When the timeout value is reached, the dynamic access list is removed, and subsequent packets (possibly valid ones) are not permitted.

Use the same inspection name in multiple statements to group them into one set of rules. This set of rules can be activated elsewhere in the configuration by using the **ip inspect inspection-name {in | out**} command when you configure an interface at the firewall.

For additional information about configuring a Cisco IOS Firewall, see *Cisco IOS Security Configuration Guide: Securing the Data Plane, Release 12.4T*.

The Cisco IOS Firewall may also be configured to provide voice security in Session Initiated Protocol (SIP) applications. SIP inspection provides basic inspect functionality (SIP packet inspection and detection of pin-hole openings), as well protocol conformance and application security. For more information, see *Cisco IOS Firewall: SIP Enhancements: ALG and AIC*.

Configuring Cisco IOS IPS

Cisco IOS Intrusion Prevention System (IPS) technology is available on Cisco 880 series ISRs and enhances perimeter firewall protection by taking appropriate action on packets and flows that violate the security policy or represent malicious network activity.

Cisco IOS IPS identifies attacks using “signatures” to detect patterns of misuse in network traffic. Cisco IOS IPS acts as an in-line intrusion detection sensor, watching packets and sessions as they flow through the router, scanning each to match known IPS signatures. When Cisco IOS IPS detects suspicious activity, it responds before network security can be compromised, it logs the event, and, depending on configuration, it does one of the following:

- Sends an alarm
- Drops suspicious packets
- Resets the connection
- Denies traffic from the source IP address of the attacker for a specified amount of time
- Denies traffic on the connection for which the signature was seen for a specified amount of time

For additional information about configuring Cisco IOS IPS, see *Cisco IOS Security Configuration Guide: Securing the Data Plane, Release 12.4T*.

URL Filtering

Cisco 860 series and Cisco 880 series ISRs provide category based URL filtering. The user provisions URL filtering on the ISR by selecting categories of websites to be permitted or blocked. An external server, maintained by a third party, is used to check for URLs in each category. Permit and deny policies are maintained on the ISR. The service is subscription based, and the URLs in each category are maintained by the third-party vendor.

For additional information about configuring URL filtering, see *Subscription-based Cisco IOS Content Filtering guide*.

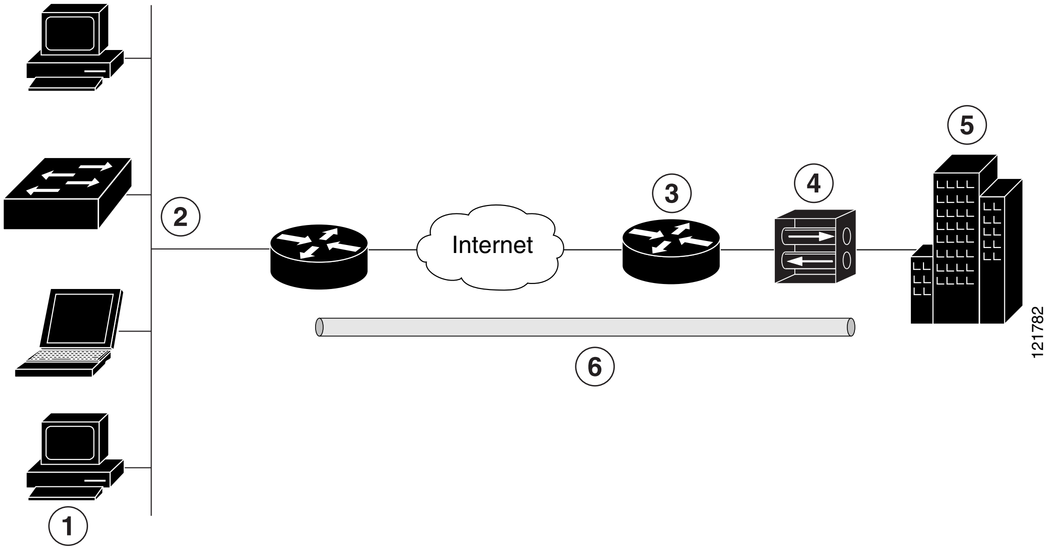
Configuring VPN

A VPN connection provides a secure connection between two networks over a public network such as the Internet. Cisco 860 and Cisco 880 series ISRs support two types of VPNs; site-to-site and remote access. Site-to-site VPNs are used to connect branch offices to corporate offices, for example. Remote access VPNs are used by remote clients to log into a corporate network. Two examples are given in this section: remote access VPN and site-to-site VPN.

Remote Access VPN

The configuration of a remote access VPN uses Cisco Easy VPN and an IP Security (IPSec) tunnel to configure and secure the connection between the remote client and the corporate network. Figure 5-1 shows a typical deployment scenario.

Figure 5-1 Remote Access VPN Using IPSec Tunnel



1	Remote networked users
2	VPN client—Cisco 880 series access router
3	Router—Providing the corporate office network access
4	VPN server—Easy VPN server; for example, a Cisco VPN 3000 concentrator with outside interface address 210.110.101.1
5	Corporate office with a network address of 10.1.1.1
6	IPSec tunnel

The Cisco Easy VPN client feature eliminates much of the tedious configuration work by implementing the Cisco Unity Client protocol. This protocol allows most VPN parameters, such as internal IP addresses, internal subnet masks, DHCP server addresses, Windows Internet Naming Service (WINS) server addresses, and split-tunneling flags to be defined at a VPN server, such as a Cisco VPN 3000 series concentrator that is acting as an IPSec server.

A Cisco Easy VPN server-enabled device can terminate VPN tunnels initiated by mobile and remote workers who are running Cisco Easy VPN Remote software on PCs. Cisco Easy VPN server-enabled devices allow remote routers to act as Cisco Easy VPN Remote nodes.

The Cisco Easy VPN client feature can be configured in one of two modes: client mode or network extension mode. Client mode is the default configuration and allows only devices at the client site to access resources at the central site. Resources at the client site are unavailable to the central site. Network extension mode allows users at the central site (where the VPN 3000 series concentrator is located) to access network resources on the client site.

After the IPSec server has been configured, a VPN connection can be created with minimal configuration on an IPSec client, such as a supported Cisco 880 series ISR. When the IPSec client initiates the VPN tunnel connection, the IPSec server pushes the IPSec policies to the IPSec client and creates the corresponding VPN tunnel connection.

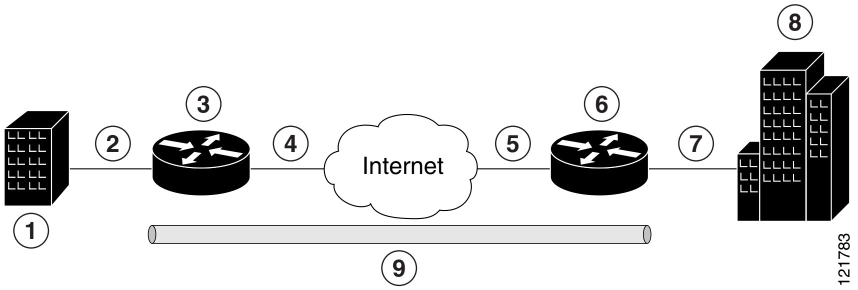
Note The Cisco Easy VPN client feature supports configuration of only one destination peer. If your application requires creation of multiple VPN tunnels, you must manually configure the IPSec VPN and Network Address Translation/Peer Address Translation (NAT/PAT) parameters on both the client and the server.

Cisco 860 and Cisco 880 series ISRs can also be configured to act as Cisco Easy VPN servers, letting authorized Cisco Easy VPN clients establish dynamic VPN tunnels to the connected network. For information on the configuration of Cisco Easy VPN servers see *Easy VPN Server*.

Site-to-Site VPN

The configuration of a site-to-site VPN uses IPSec and the generic routing encapsulation (GRE) protocol to secure the connection between the branch office and the corporate network. Figure 5-2 shows a typical deployment scenario.

Figure 5-2 Site-to-Site VPN Using an IPSec Tunnel and GRE



1	Branch office containing multiple LANs and VLANs
2	Fast Ethernet LAN interface—With address 192.165.0.0/16 (also the inside interface for NAT)
3	VPN client—Cisco 860 or Cisco 880 series ISR
4	Fast Ethernet or ATM interface—With address 200.1.1.1 (also the outside interface for NAT)

5	LAN interface—Connects to the Internet; with outside interface address of 210.110.101.1
6	VPN client—Another router, which controls access to the corporate network
7	LAN interface—Connects to the corporate network, with inside interface address of 10.1.1.1
8	Corporate office network
9	IPSec tunnel with GRE

For more information about IPSec and GRE configuration, see *Cisco IOS Security Configuration Guide: Secure Connectivity, Release 12.4T*.

Configuration Examples

Each example configures a VPN over an IPSec tunnel, using the procedure given in the "Configure a VPN over an IPSec Tunnel" section on page 5-7. The specific procedure for a remote access configuration is given, followed by the specific procedure for a site-to-site configuration.

The examples shown in this chapter apply only to the endpoint configuration on the Cisco 860 and Cisco 880 ISRs. Any VPN connection requires both endpoints be configured properly to function. See the software configuration documentation as needed to configure the VPN for other router models.

VPN configuration information must be configured on both endpoints. You must specify parameters, such as internal IP addresses, internal subnet masks, DHCP server addresses, and Network Address Translation (NAT).

- Configure a VPN over an IPSec Tunnel, page 5-7
- Create a Cisco Easy VPN Remote Configuration, page 5-14
- Configure a Site-to-Site GRE Tunnel, page 5-17

Configure a VPN over an IPSec Tunnel

Perform the following tasks to configure a VPN over an IPSec tunnel:

- Configure the IKE Policy, page 5-8
- Configure Group Policy Information, page 5-9
- Apply Mode Configuration to the Crypto Map, page 5-10
- Enable Policy Lookup, page 5-11
- Configure IPSec Transforms and Protocols, page 5-12
- Configure the IPSec Crypto Method and Parameters, page 5-13
- Apply the Crypto Map to the Physical Interface, page 5-14
- Where to Go Next, page 5-14

Configure the IKE Policy

To configure the Internet Key Exchange (IKE) policy, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **crypto isakmp policy** *priority*
2. **encryption** {**des** | **3des** | **aes** | **aes 192** | **aes 256**}
3. **hash** {**md5** | **sha**}
4. **authentication** {**rsa-sig** | **rsa-encr** | **pre-share**}
5. **group** {**1** | **2** | **5**}
6. **lifetime** *seconds*
7. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	**crypto isakmp policy** *priority* **Example:** `Router(config)# crypto isakmp policy 1`	Creates an IKE policy that is used during IKE negotiation. The priority is a number from 1 to 10000, with 1 being the highest. Also enters the Internet Security Association Key and Management Protocol (ISAKMP) policy configuration mode.

Step 2	**encryption** {**des** | **3des** | **aes** | **aes 192** | **aes 256**}
	Example:
	`Router(config-isakmp)# encryption 3des`
		Specifies the encryption algorithm used in the IKE policy.
		The example specifies 168-bit data encryption standard (DES).

Step 3	**hash** {**md5** | **sha**}
	Example:
	`Router(config-isakmp)# hash md5`
		Specifies the hash algorithm used in the IKE policy.
		The example specifies the Message Digest 5 (MD5) algorithm. The default is Secure Hash standard (SHA-1).

Step 4	**authentication** {**rsa-sig** | **rsa-encr** | **pre-share**}
	Example:
	`Router(config-isakmp)# authentication pre-share`
		Specifies the authentication method used in the IKE policy.
		The example specifies a pre-shared key.

Step 5	**group** {**1** | **2** | **5**}
	Example:
	`Router(config-isakmp)# group 2`
		Specifies the Diffie-Hellman group to be used in an IKE policy.

	Command	Purpose
Step 6	**lifetime** *seconds* **Example:** `Router(config-isakmp)# lifetime 480`	Specifies the lifetime, in seconds, for an IKE security association (SA). Acceptable values are from 60 to 86400.
Step 7	**exit** **Example:** `Router(config-isakmp)# exit`	Exits ISAKMP policy configuration mode and returns to global configuration mode.

Configure Group Policy Information

To configure the group policy, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **crypto isakmp client configuration group** {**group-name** | **default**}
2. **key** *name*
3. **dns** *primary-server*
4. **domain** *name*
5. **exit**
6. **ip local pool** {**default** | *poolname*} [*low-ip-address* [*high-ip-address*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**crypto isakmp client configuration group** {**group-name** | **default**} **Example:** `Router(config)# crypto isakmp client configuration group rtr-remote`	Creates an IKE policy group containing attributes to be downloaded to the remote client. Also enters the Internet Security Association Key and Management Protocol (ISAKMP) group policy configuration mode.
Step 2	**key** *name* **Example:** `Router(config-isakmp-group)# key secret-password`	Specifies the IKE pre-shared key for the group policy.
Step 3	**dns** *primary-server* **Example:** `Router(config-isakmp-group)# dns 10.50.10.1`	Specifies the primary Domain Name System (DNS) server for the group. **Note** To specify Windows Internet Naming Service (WINS) servers for the group, use the **wins** command.

	Command or Action	Purpose
Step 4	**domain** *name* **Example:** `Router(config-isakmp-group)# domain company.com`	Specifies group domain membership.

Step 5	**exit**
	Example:
	`Router(config-isakmp-group)# exit`
	`Router(config)#`
		Exits ISAKMP group policy configuration mode and returns to global configuration mode.

Step 6	**ip local pool** {**default** | *poolname*} [*low-ip-address* [*high-ip-address*]] **Example:** `Router(config)# ip local pool dynpool 30.30.30.20 30.30.30.30`	Specifies a local address pool for the group. For details about this command and additional parameters that can be set, see *Cisco IOS Dial Technologies Command Reference*.

Apply Mode Configuration to the Crypto Map

To apply mode configuration to the crypto map, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **crypto map** *map-name* **isakmp authorization list** *list-name*
2. **crypto map** *tag* **client configuration address** [**initiate** | **respond**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**crypto map** *map-name* **isakmp authorization list** *list-name* **Example:** `Router(config)# crypto map dynmap isakmp authorization list rtr-remote`	Applies mode configuration to the crypto map and enables key lookup (IKE queries) for the group policy from an authentication, authorization, and accounting (AAA) server.
Step 2	**crypto map** *tag* **client configuration address** [**initiate** | **respond**] **Example:** `Router(config)# crypto map dynmap client configuration address respond`	Configures the router to reply to mode configuration requests from remote clients.

Enable Policy Lookup

To enable policy lookup through AAA, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **aaa new-model**
2. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
3. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2...*]]
4. **username** *name* {**nopassword** | **password** *password* | **password** *encryption-type encrypted-password*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables the AAA access control model.
Step 2	**aaa authentication login** {**default**	*list-name*} *method1* [*method2...*] **Example:** `Router(config)# aaa authentication login rtr-remote local`	Specifies AAA authentication of selected users at login, and specifies the method used. • This example uses a local authentication database. **Note** You could also use a RADIUS server. For details, see *Cisco IOS Security Configuration Guide: Securing User Services, Release 12.4T* and *Cisco IOS Security Command Reference*.
Step 3	**aaa authorization** {**network**	**exec**	**commands** *level*	**reverse-access**	**configuration**} {**default**	*list-name*} [*method1* [*method2...*]] **Example:** `Router(config)# aaa authorization network rtr-remote local`	Specifies AAA authorization of all network-related service requests, including PPP, and specifies the method of authorization. • This example uses a local authorization database. **Note** You could also use a RADIUS server. For details, see *Cisco IOS Security Configuration Guide: Securing User Services, Release 12.4T* and *Cisco IOS Security Command Reference*.

Step 4	**username** *name* {**nopassword**	**password** *password*	**password** *encryption-type encrypted-password*}
			Example:
			`Router(config)# username username1 password 0 password1`
				Establishes a username-based authentication system.

Configure IPSec Transforms and Protocols

A transform set represents a certain combination of security protocols and algorithms. During IKE negotiation, the peers agree to use a particular transform set for protecting data flow.

During IKE negotiations, the peers search in multiple transform sets for a transform that is the same at both peers. When a transform set is found that contains such a transform, it is selected and applied to the protected traffic as a part of both configurations.

To specify the IPSec transform set and protocols, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **crypto ipsec profile** *profile-name*
2. **crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]
3. **crypto ipsec security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**crypto ipsec profile** *profile-name* **Example:** `Router(config)# crypto ipsec profile pro1`	Configures IPSec profile to apply protection on the tunnel for encryption.
Step 2	**crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*] **Example:** `Router(config)# crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac`	Defines a transform set—an acceptable combination of IPSec security protocols and algorithms. See *Cisco IOS Security Configuration Guide: Secure Connectivity, Release 12.4T* for details about the valid transforms and combinations.

Step 3	**crypto ipsec security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}
	Example:
	`Router(config)# crypto ipsec security-association lifetime seconds 86400`
		Specifies global lifetime values used when IPSec security associations are negotiated.

Configure the IPSec Crypto Method and Parameters

A dynamic crypto map policy processes negotiation requests for new security associations from remote IPSec peers, even if the router does not know all the crypto map parameters (for example, IP address).

To configure the IPSec crypto method, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **crypto dynamic-map** *dynamic-map-name dynamic-seq-num*
2. **set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*]
3. **reverse-route**
4. **exit**
5. **crypto map** *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**crypto dynamic-map** *dynamic-map-name dynamic-seq-num* **Example:** `Router(config)# crypto dynamic-map dynmap 1`	Creates a dynamic crypto map entry and enters crypto map configuration mode. See *Cisco IOS Security Command Reference* for more details about this command.
Step 2	**set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*] **Example:** `Router(config-crypto-map)# set transform-set vpn1`	Specifies which transform sets can be used with the crypto map entry.
Step 3	**reverse-route** **Example:** `Router(config-crypto-map)# reverse-route`	Creates source proxy information for the crypto map entry. See *Cisco IOS Security Command Reference* for details.
Step 4	**exit** **Example:** `Router(config-crypto-map)# exit`	Exits crypto map configuration mode and returns to global configuration mode.
Step 5	**crypto map** *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*] **Example:** `Router(config)# crypto map static-map 1 ipsec-isakmp dynamic dynmap`	Creates a crypto map profile.

Apply the Crypto Map to the Physical Interface

The crypto maps must be applied to each interface through which IPSec traffic flows. Applying the crypto map to the physical interface instructs the router to evaluate all the traffic against the security associations database. With the default configurations, the router provides secure connectivity by encrypting the traffic sent between remote sites. However, the public interface still allows the rest of the traffic to pass and provides connectivity to the Internet.

To apply a crypto map to an interface, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **interface** *type number*
2. **crypto map** *map-name*
3. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface** *type number* **Example:** `Router(config)# interface fastethernet 4`	Enters the interface configuration mode for the interface to which the crypto map will be applied.
Step 2	**crypto map** *map-name* **Example:** `Router(config-if)# crypto map static-map`	Applies the crypto map to the interface. • See *Cisco IOS Security Command Reference* for more details about this command.

Step 3	**exit**
	Example:
	`Router(config-crypto-map)# exit`
	`Router(config)#`
		Exits interface configuration mode and returns to global configuration mode.

Where to Go Next

If you are creating a Cisco Easy VPN remote configuration, go to the "Create a Cisco Easy VPN Remote Configuration" section on page 5-14.

If you are creating a site-to-site VPN using IPSec tunnels and GRE, go to the "Configure a Site-to-Site GRE Tunnel" section on page 5-17.

Create a Cisco Easy VPN Remote Configuration

The router acting as the Cisco Easy VPN client must create a Cisco Easy VPN remote configuration and assign it to the outgoing interface.

To create the remote configuration, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **crypto ipsec client ezvpn** *name*
2. **group** *group-name* **key** *group-key*
3. **peer** {*ipaddress* | *hostname*}
4. **mode** {**client** | **network-extension** | **network extension plus**}
5. **exit**
6. **crypto isakmp keepalive** *seconds*
7. **interface** *type number*
8. **crypto ipsec client ezvpn** *name* [**outside** | **inside**]
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**crypto ipsec client ezvpn** *name* **Example:** `Router(config)# crypto ipsec client ezvpn ezvpnclient`	Creates a Cisco Easy VPN remote configuration, and enters Cisco Easy VPN remote configuration mode.
Step 2	**group** *group-name* **key** *group-key* **Example:** `Router(config-crypto-ezvpn)# group ezvpnclient key secret-password`	Specifies the IPSec group and IPSec key value for the VPN connection.

Step 3	**peer** {*ipaddress*	*hostname*}
		Example:
		`Router(config-crypto-ezvpn)# peer 192.168.100.1`
			Specifies the peer IP address or hostname for the VPN connection.
			• A hostname can be specified only when the router has a DNS server available for hostname resolution.
			Note Use this command to configure multiple peers for use as backup. If one peer goes down, the Easy VPN tunnel is established with the second available peer. When the primary peer comes up again, the tunnel is reestablished with the primary peer.

Step 4	**mode** {**client**	**network-extension**	**network extension plus**}
			Example:
			`Router(config-crypto-ezvpn)# mode client`
				Specifies the VPN mode of operation.

Step 5	**exit** **Example:** `Router(config-crypto-ezvpn)# exit`	Exits Cisco Easy VPN remote configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 6	**crypto isakmp keepalive** *seconds* **Example:** `Router(config)# crypto isakmp keepalive 10`	Enables dead peer detection messages. • *seconds*—Sets the time between messages. The range is from 10 to 3600.
Step 7	**interface** *type number* **Example:** `Router(config)# interface fastethernet 4`	Enters the interface configuration mode for the interface to which the Cisco Easy VPN remote configuration will be applied. **Note** For routers with an ATM WAN interface, this command would be **interface atm 0**.
Step 8	**crypto ipsec client ezvpn** *name* [**outside** | **inside**] **Example:** `Router(config-if)# crypto ipsec client ezvpn ezvpnclient outside`	Assigns the Cisco Easy VPN remote configuration to the WAN interface. • This command causes the router to automatically create the NAT or port address translation (PAT) and access list configuration needed for the VPN connection.
Step 9	**exit** **Example:** `Router(config-crypto-ezvpn)# exit`	Exits interface configuration mode and returns to global configuration mode.

Configuration Example

The following configuration example shows a portion of the configuration file for the VPN and IPSec tunnel described in this chapter.

```
!
aaa new-model
!
aaa authentication login rtr-remote local
aaa authorization network rtr-remote local
aaa session-id common
!
username Cisco password 0 Cisco
!
crypto isakmp policy 1
    encryption 3des
    authentication pre-share
    group 2
    lifetime 480
!
crypto isakmp client configuration group rtr-remote
    key secret-password
    dns 10.50.10.1 10.60.10.1
    domain company.com
    pool dynpool
!
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
!
crypto ipsec security-association lifetime seconds 86400
!
crypto dynamic-map dynmap 1
    set transform-set vpn1
    reverse-route
!
```

```
crypto map static-map 1 ipsec-isakmp dynamic dynmap
crypto map dynmap isakmp authorization list rtr-remote
crypto map dynmap client configuration address respond

crypto ipsec client ezvpn ezvpnclient
    connect auto
    group 2 key secret-password
    mode client
    peer 192.168.100.1
!

interface fastethernet 4
    crypto ipsec client ezvpn ezvpnclient outside
    crypto map static-map
!
interface vlan 1
    crypto ipsec client ezvpn ezvpnclient inside
!
```

Configure a Site-to-Site GRE Tunnel

To configure a GRE tunnel, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **interface** *type number*
2. **ip address** *ip-address mask*
3. **tunnel source** *interface-type number*
4. **tunnel destination** *default-gateway-ip-address*
5. **crypto map** *map-name*
6. **exit**
7. **ip access-list** {**standard** | **extended**} *access-list-name*
8. **permit** *protocol source source-wildcard destination destination-wildcard*
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface** *type number* **Example:** `Router(config)# interface tunnel 1`	Creates a tunnel interface and enters interface configuration mode.
Step 2	**ip address** *ip-address mask* **Example:** `Router(config-if)# 10.62.1.193 255.255.255.252`	Assigns an address to the tunnel.

	Command or Action	Purpose
Step 3	**tunnel source** *interface-type number* **Example:** `Router(config-if)# tunnel source fastethernet 0`	Specifies the source endpoint of the router for the GRE tunnel.
Step 4	**tunnel destination** *default-gateway-ip-address* **Example:** `Router(config-if)# tunnel destination 192.168.101.1`	Specifies the destination endpoint of the router for the GRE tunnel.
Step 5	**crypto map** *map-name* **Example:** `Router(config-if)# crypto map static-map`	Assigns a crypto map to the tunnel. **Note** Dynamic routing or static routes to the tunnel interface must be configured to establish connectivity between the sites.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode, and returns to global configuration mode.
Step 7	**ip access-list** {**standard** | **extended**} *access-list-name* **Example:** `Router(config)# ip access-list extended vpnstatic1`	Enters ACL configuration mode for the named ACL that is used by the crypto map.
Step 8	**permit** *protocol source source-wildcard destination destination-wildcard* **Example:** `Router(config-acl)# permit gre host 192.168.100.1 host 192.168.101.1`	Specifies that only GRE traffic is permitted on the outbound interface.

Step 9	**exit**
	Example:
	`Router(config-acl)# exit`
	`Router(config)#`
		Exits ACL configuration mode and returns to global configuration mode.

Configuration Example

The following configuration example shows a portion of the configuration file for a VPN using a GRE tunnel scenario described in the preceding sections.

```
!
aaa new-model
!
aaa authentication login rtr-remote local
aaa authorization network rtr-remote local
aaa session-id common
!
username cisco password 0 cisco
!
```

```
interface tunnel 1
    ip address 10.62.1.193 255.255.255.252

tunnel source fastethernet 0

tunnel destination interface 192.168.101.1

ip route 20.20.20.0 255.255.255.0 tunnel 1

crypto isakmp policy 1
    encryption 3des
    authentication pre-share
    group 2
!
crypto isakmp client configuration group rtr-remote
    key secret-password
    dns 10.50.10.1 10.60.10.1
    domain company.com
    pool dynpool
!
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
!
crypto ipsec security-association lifetime seconds 86400
!
crypto dynamic-map dynmap 1
    set transform-set vpn1
    reverse-route
!
crypto map static-map 1 ipsec-isakmp dynamic dynmap
crypto map dynmap isakmp authorization list rtr-remote
crypto map dynmap client configuration address respond
!
! Defines the key association and authentication for IPsec tunnel.
crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key cisco123 address 200.1.1.1
!
!
! Defines encryption and transform set for the IPsec tunnel.
crypto ipsec transform-set set1 esp-3des esp-md5-hmac
!
! Associates all crypto values and peering address for the IPsec tunnel.
crypto map to_corporate 1 ipsec-isakmp
 set peer 200.1.1.1
 set transform-set set1
 match address 105
!
!
! VLAN 1 is the internal home network.
interface vlan 1
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 ip inspect firewall in ! Inspection examines outbound traffic.
 crypto map static-map
 no cdp enable
!
! FE4 is the outside or Internet-exposed interface
interface fastethernet 4
 ip address 210.110.101.21 255.255.255.0
 ! acl 103 permits IPsec traffic from the corp. router as well as
 ! denies Internet-initiated traffic inbound.
 ip access-group 103 in
 ip nat outside
 no cdp enable
 crypto map to_corporate ! Applies the IPsec tunnel to the outside interface.
!
! Utilize NAT overload in order to make best use of the
! single address provided by the ISP.
ip nat inside source list 102 interface Ethernet1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 210.110.101.1
no ip http server
!
!
! acl 102 associated addresses used for NAT.
access-list 102 permit ip 10.1.1.0 0.0.0.255 any
! acl 103 defines traffic allowed from the peer for the IPsec tunnel.
access-list 103 permit udp host 200.1.1.1 any eq isakmp
access-list 103 permit udp host 200.1.1.1 eq isakmp any
access-list 103 permit esp host 200.1.1.1 any
! Allow ICMP for debugging but should be disabled because of security implications.
access-list 103 permit icmp any any
access-list 103 deny ip any any ! Prevents Internet-initiated traffic inbound.
! acl 105 matches addresses for the IPsec tunnel to or from the corporate network.
access-list 105 permit ip 10.1.1.0 0.0.0.255 192.168.0.0 0.0.255.255
no cdp run
```

CHAPTER 6

Configuring Backup Data Lines and Remote Management

This chapter describes configuring backup data lines and remote management in the following sections:

- Configuring Backup Interfaces, page 6-2
- Configuring Cellular Dial-on-Demand Routing Backup, page 6-3
- Configuring Dial Backup and Remote Management Through the Console or Auxiliary Port, page 6-10
- Configuring Data Line Backup and Remote Management Through the ISDN S/T Port, page 6-15
- Configuring Gigabit Ethernet Failover Media, page 6-20
- Configuring Third-Party SFPs, page 6-22

The Cisco 880 Series Integrated Services Routers (ISRs) support backup data connectivity with a backup data line that enables them to mitigate WAN downtime.

Note Voice backup is available on router models C881SRST and C888SRST. For information on configuring voice backup, see Chapter 8, "Configuring Voice Functionality."

Cisco 880 ISRs also support remote management functions as follows:

- Through the auxiliary port on any Cisco 880 series ISRs
- Through the ISDN S/T port on the Cisco 880 series ISRs

Note On the Cisco 880 series ISRs, the console port and the auxiliary port are on the same physical RJ-45 port; therefore, the two ports cannot be activated simultaneously. You must use the CLI to enable the desired function.

Cisco 892F ISRs have a Gigabit Ethernet (GE) port that supports copper connections or a small-form-factor pluggable (SFP) port that supports fiber connections and can be configured for failover redundancy when the network goes down.

Configuring Backup Interfaces

When the router receives an indication that the primary interface is down, the backup interface becomes enabled. After the primary connection has been restored for a specified period, the backup interface is disabled.

Even if the backup interface comes out of standby mode, the router does not enable the backup interface unless the router receives the traffic specified for that backup interface.

Table 6-1 shows the backup interfaces for Cisco 880 and Cisco 890 series ISRs, along with their port designations. Basic configurations for these interfaces are given in the "Configuring WAN Interfaces" section on page 3-8 of Chapter 3, "Basic Router Configuration."

Table 6-1 Model Numbers and Data Line Backup Capabilities

Router Model Number	ISDN	3G	V.92
881G, 886G, 887G, 887VG, 888G	—	Yes	—
886, 886VA, 887, 887V, 888, 888E	Yes	—	—
891	—	—	Yes
892, 892F	Yes	—	—

To configure your router with a backup interface, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **interface** *type number*
2. **backup interface** *interface-type interface-number*
3. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	**interface** *type number* **Example:** `Router(config)# interface atm 0`	Enters interface configuration mode for the interface for which you want to configure the backup. This interface can be a serial, ISDN, or asynchronous. The example shows the configuration of a backup interface for an ATM WAN connection.

	Command	Purpose
Step 2	**backup interface** *interface-type interface-number* **Example:** `Router(config-if)# backup interface bri 0`	Assigns an interface as the secondary, or backup interface. This can be a serial interface or asynchronous interface. For example, a serial 1 interface could be configured to back up a serial 0 interface. The example shows a BRI interface configured as the backup interface for the ATM 0 interface.

Step 3	**exit**
	Example:
	`Router(config-if)# exit`
	`Router(config)#`
		Exits the configuration interface mode.

Configuring Cellular Dial-on-Demand Routing Backup

To monitor the primary connection and initiate the backup connection over the cellular interface when needed, the router can use one of the following methods:

- Backup Interface—Backup interface that stays in standby mode until the primary interface line protocol is detected as down and then is brought up. See the "Configuring Backup Interfaces" section on page 6-2.
- Dialer Watch—Backup feature that integrates dial backup with routing capabilities. See the "Configuring DDR Backup Using Dialer Watch" section on page 6-4.
- Floating Static Route—Route through the backup interface has an administrative distance that is greater than the administrative distance of the primary connection route and therefore would not be in the routing table until the primary interface goes down. When the primary interaface goes down, the floating static route is used. See the "Configuring DDR Backup Using Floating Static Route" section on page 6-5

Note You cannot configure a backup interface for the cellular interface and any other asynchronous serial interface.

Configuring DDR Backup Using Dialer Watch

To initiate dialer watch, you must configure the interface to perform dial-on-demand routing (DDR) and backup. Use traditional DDR configuration commands, such as dialer maps, for DDR capabilities. To enable dialer watch on the backup interface and create a dialer list, use the following commands in interface configuration mode.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *type number*
3. **dialer watch group** *group-number*
4. **dialer watch-list** *group-number* **ip** *ip-address address-mask*
5. **dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | **access-group**}
6. **ip access-list** *access-list-number* **permit** *ip source address*
7. **interface cellular** *0*
8. **dialer string** *string*

   or

   dialer group *dialer group number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**interface** *type number* **Example:** `Router (config)# interface ATM0`	Specifies the interface.
Step 3	**dialer watch-group** *group-number* **Example:** `Router(config-if)# dialer watch-group 2`	Enables dialer watch on the backup interface.
Step 4	**dialer watch-list** *group-number* **ip** *ip-address address-mask* **Example:** `Router(config-if)# dialer watch-list 2 ip 10.4.0.254 255.255.0.0`	Defines a list of all IP addresses to be watched.

	Command or Action	Purpose

Step 5	**dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | **access-group**}
	Example:
	`Router(config)# dialer-list 2 protocol ip permit`
		Creates a dialer list for traffic of interest and permits access to an entire protocol.

Step 6	**ip access-list** *access-list-number* **permit** *ip source address* **Example:** `Router(config)# access list 2 permit 10.4.0.0`	Defines traffic of interest. Do not use the **access list permit all** command to avoid sending traffic to the IP network. This may result in call termination.

Step 7	**`interface cellular`** ***`0`***
	Example:
	`Router (config)# interface cellular 0`
		Specifies the cellular interface.

Step 8	**dialer string** *string*
	or
	dialer group *dialer group number*
	Example:
	`Router (config-if)# dialer string cdma  *** cdma ***`
	or
	`Router (config-if)# dialer group 2      *** gsm ***`
		CDMA only. Specifies the dialer script (defined using the **chat script** command).
		GSM only. Maps a dialer list to the dialer interface.

Configuring DDR Backup Using Floating Static Route

To configure a floating static default route on the secondary interface, use the following commands, beginning in the global configuration mode.

Note Make sure you have ip classless enabled on your router.

SUMMARY STEPS

1. **configure terminal**
2. **ip route** *network-number network-mask* {*ip address* | *interface*} [*administrative distance*] [**name** *name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode from the terminal.
Step 2	**ip route** *network-number network-mask* {*ip address* | *interface*} [*administrative distance*] [**name** *name*] **Example:** `Router (config)# ip route 0.0.0.0 Dialer 2 track 234`	Establishes a floating static route with the configured administrative distance through the specified interface. A higher administrative distance should be configured for the route through the backup interface, so that the backup interface is used only when the primary interface is down.

Cellular Wireless Modem as Backup with NAT and IPsec Configuration

The following example shows how to configure the 3G wireless modem as backup with NAT and IPsec on either GSM or CDMA networks.

Note The receive and transmit speeds cannot be configured. The actual throughput depends on the cellular network service.

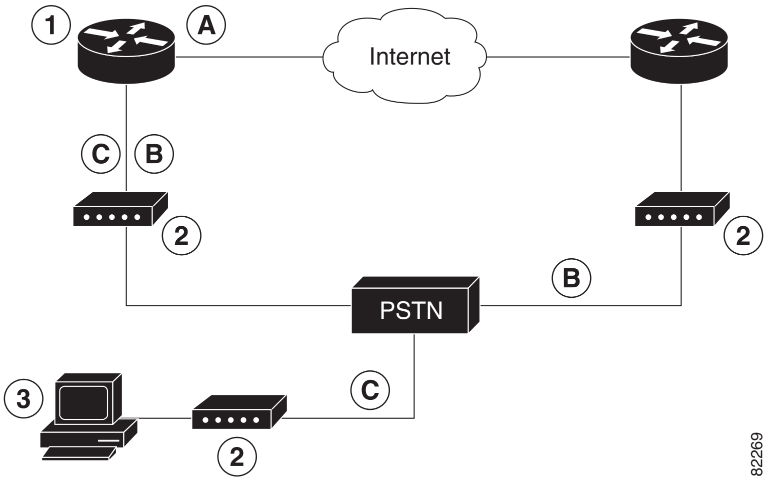
```
Current configuration : 3433 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
!
!
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
crypto isakmp key gsm address 128.107.241.234              *** or cdma ***
!
!
crypto ipsec transform-set gsm ah-sha-hmac esp-3des        *** or cdma ***
!
crypto map gsm1 10 ipsec-isakmp                            *** or cdma1 ***
 set peer 128.107.241.234
 set transform-set gsm                                     *** or cdma ***
 match address 103
!
!
!
no ip dhcp use vrf connected
ip dhcp excluded-address 10.4.0.254
!
ip dhcp pool gsmpool                                        *** or cdmapool ***
   network 10.4.0.0 255.255.0.0
   dns-server 66.209.10.201 66.102.163.231
   default-router 10.4.0.254
!
!
ip cef
!
no ipv6 cef
multilink bundle-name authenticated
chat-script gsm "" "atdt*98*1#" TIMEOUT 30 "CONNECT"        *** or cdma ***
!
!
archive
 log config
  hidekeys
!
!
controller DSL 0
 mode atm
 line-term cpe
 line-mode 4-wire standard
 line-rate 4608
!
!
!
!
interface ATM0
 no ip address
 ip virtual-reassembly
 load-interval 30
 no atm ilmi-keepalive
!
interface ATM0.1 point-to-point
 backup interface Cellular0
 ip nat outside
 ip virtual-reassembly
 pvc 0/35
  pppoe-client dial-pool-number 2
 !
!
interface FastEthernet0
!
interface FastEthernet1
!
interface FastEthernet2
!
interface FastEthernet3
!
interface Cellular0
 ip address negotiated
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
 no ip mroute-cache
 dialer in-band
 dialer idle-timeout 0
 dialer string gsm                                      *** or cdma ***
 dialer-group 1
 async mode interactive
 no ppp lcp fast-start
 ppp chap hostname chunahayev@wwan.ccs
 ppp chap password 0 B7uhestacr
 ppp ipcp dns request
 crypto map gsm1                                       *** or cdma1 ***
!
interface Vlan1
 description used as default gateway address for DHCP clients
 ip address 10.4.0.254 255.255.0.0
 ip nat inside
 ip virtual-reassembly
!
interface Dialer2
 ip address negotiated
 ip mtu 1492
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
 load-interval 30
 dialer pool 2
 dialer-group 2
 ppp authentication chap callin
 ppp chap hostname cisco@dsl.com
 ppp chap password 0 cisco
 ppp ipcp dns request
 crypto map gsm1                                       *** or cdma1 ***
!
ip local policy route-map track-primary-if
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 Dialer2 track 234
ip route 0.0.0.0 0.0.0.0 Cellular0 254
no ip http server
no ip http secure-server
!
!
ip nat inside source route-map nat2cell interface Cellular0 overload
ip nat inside source route-map nat2dsl interface Dialer2 overload
!
ip sla 1
 icmp-echo 209.131.36.158 source-interface Dialer2
 timeout 1000
 frequency 2
ip sla schedule 1 life forever start-time now
access-list 1 permit any
access-list 2 permit 10.4.0.0 0.0.255.255
access-list 3 permit any
access-list 101 permit ip 10.4.0.0 0.0.255.255 any
access-list 102 permit icmp any host 209.131.36.158
access-list 103 permit ip host 166.136.225.89 128.107.0.0 0.0.255.255
access-list 103 permit ip host 75.40.113.246 128.107.0.0 0.0.255.255
dialer-list 1 protocol ip list 1
dialer-list 2 protocol ip permit
!
!
!
route-map track-primary-if permit 10
 match ip address 102
 set interface Dialer2
!
route-map nat2dsl permit 10
 match ip address 101
 match interface Dialer2
!
route-map nat2cell permit 10
 match ip address 101
 match interface Cellular0
!
!
control-plane
!
!
line con 0
 no modem enable
line aux 0
line 3
 exec-timeout 0 0
 script dialer gsm                                       *** or cdma ***
 login
 modem InOut
 no exec
line vty 0 4
 login
!
scheduler max-task-time 5000

!
webvpn cef
end
```

Configuring Dial Backup and Remote Management Through the Console or Auxiliary Port

When customer premises equipment, such as a Cisco 880 series ISR, is connected to an ISP, an IP address is dynamically assigned to the router, or the IP address may be assigned by the router peer through the centrally managed function. The dial backup feature can be added to provide a failover route in case the primary line fails. The Cisco 880 series ISRs can use the auxiliary port for dial backup and remote management.

Figure 6-1 shows the network configuration used for remote management access and for providing backup to the primary WAN line.

Figure 6-1 Dial Backup and Remote Management Through the Auxiliary Port



1	Cisco 880 series router	**A**	Main WAN link; primary connection to Internet service provider
2	Modem	**B**	Dial backup; serves as a failover link for Cisco 880 routers when the primary line goes down
3	PC	**C**	Remote management; serves as dial-in access to allow changes or updates to Cisco IOS configurations

To configure dial backup and remote management for these routers, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **ip name-server** *server-address*
2. **ip dhcp pool** *name*
3. **exit**
4. **chat-script** *script-name expect-send*
5. **interface** *type number*
6. **exit**

7. **interface** *type number*
8. **dialer watch-group** *group-number*
9. **exit**
10. **ip nat inside source {list** *access-list-number***} {interface** *type number* **| pool** *name***} [overload]**
11. **ip route** *prefix mask* {***ip-address*** **|** ***interface-type interface-number*** [***ip-address***]}
12. **access-list** *access-list-number* **{deny | permit}** *source* [*source-wildcard*]
13. **dialer watch-list** *group-number* {**ip** *ip-address address-mask* **| delay route-check initial** *seconds*}
14. **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]
15. **modem enable**
16. **exit**
17. **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]
18. **flowcontrol** {**none** | **software** [**lock**] [**in** | **out**] | **hardware** [**in** | **out**]}

DETAILED STEPS

	Command	Purpose
Step 1	**ip name-server** *server-address* **Example:** `Router(config)# ip name-server 192.168.28.12`	Enters your ISP DNS IP address. **Tip** You may add multiple server addresses if available.
Step 2	**ip dhcp pool** *name* **Example:** `Router(config)# ip dhcp pool 1`	Creates a DHCP address pool on the router and enters DHCP pool configuration mode. The *name* argument can be a string or an integer. Configure the DHCP address pool. For sample commands that you can use in DHCP pool configuration mode, see the "Example" section on page 6-13.
Step 3	**exit** **Example:** `Router(config-dhcp)#exit`	Exits config-dhcp mode and enters global configuration mode.
Step 4	**chat-script** *script-name expect-send* **Example:** `Router(config)# chat-script Dialout ABORT ERROR ABORT BUSY "" "AT" OK "ATDT 5555102 T" TIMEOUT 45 CONNECT \c`	Configures a chat script used in dial-on-demand routing (DDR) to give commands for dialing a modem and for logging in to remote systems. The defined script is used to place a call over a modem connected to the PSTN.
Step 5	**interface** *type number* **Example:** `Router(config)# interface Async 1`	Creates and enters configuration mode for the asynchronous interface. Configure the asynchronous interface. For sample commands that you can use in asynchronous interface configuration mode, see the "Example" section on page 6-13.

	Command	Purpose
Step 6	**exit** **Example:** `Router(config-if)# exit`	Enters global configuration mode.
Step 7	**interface** *type number* **Example:** `Router(config)# interface Dialer 3`	Creates and enters configuration mode for the dilaer interface.
Step 8	**dialer watch-group** *group-number* **Example:** `Router(config-if)# dialer watch-group 1`	Specifies the group number for the watch list.
Step 9	**exit** **Example:** `Router(config-if)# exit`	Exits the interface configuration mode.

Step 10	**ip nat inside source** {**list** *access-list-number*} {**interface** *type number* | **pool** *name*} [**overload**]
	Example:
	`Router(config)# ip nat inside source list`
	`101 interface Dialer 3 overload`
		Enables dynamic translation of addresses on the inside interface.

Step 11	**ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]}
	Example:
	`Router(config)# ip route 0.0.0.0 0.0.0.0`
	`22.0.0.2`
		Sets the IP route to point to the dialer interface as a default gateway.

Step 12	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
	Example:
	`Router(config)# access-list 1 permit`
	`192.168.0.0 0.0.255.255 any`
		Defines an extended access list that indicates which addresses need translation.

Step 13	**dialerwatch-list** *group-number* {**ip** *ip-address address-mask* | **delay route-check initial** *seconds*}
	Example:
	`Router(config)# dialer watch-list 1 ip`
	`22.0.0.2 255.255.255.255`
		Evaluates the status of the primary link, based on the existence of routes to the peer. The address 22.0.0.2 is the peer IP address of the ISP.

Step 14	**line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*] **Example:** `Router(config)# line console 0`	Enters configuration mode for the line interface.

	Command	Purpose
Step 15	**modem enable** **Example:** `Router(config-line)# modem enable`	Switches the port from console to auxiliary port function.
Step 16	**exit** **Example:** `Router(config-line)# exit`	Exits the configure interface mode.
Step 17	**line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*] **Example:** `Router(config)# line aux 0`	Enters configuration mode for the auxiliary interface.

Step 18	**flowcontrol** {**none** | **software** [**lock**] [**in** | **out**] | **hardware** [**in** | **out**]}
	Example:
	`Router(config)# flowcontrol hardware`
		Enables hardware signal flow control.

Example

The following configuration example specifies an IP address for the ATM interface through PPP and IPCP address negotiation and dial backup over the console port.

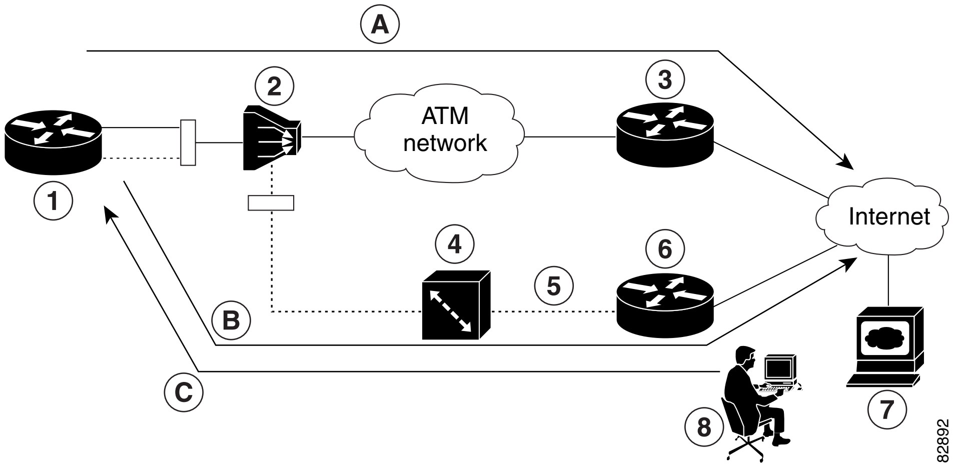
```
!
ip name-server 192.168.28.12
ip dhcp excluded-address 192.168.1.1
!
ip dhcp pool 1
 import all
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
!
! Need to use your own correct ISP phone number.
modemcap entry MY-USER_MODEM:MSC=&F1S0=1
chat-script Dialout ABORT ERROR ABORT BUSY "" "AT" OK "ATDT 5555102\T"
TIMEOUT 45 CONNECT \c
!
!
!
!
interface vlan 1
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip tcp adjust-mss 1452
 hold-queue 100 out
!
! Dial backup and remote management physical interface.
interface Async1
 no ip address
 encapsulation ppp
 dialer in-band
 dialer pool-member 3
 async default routing
 async dynamic routing
 async mode dedicated
 ppp authentication pap callin
!
interface ATM0
 mtu 1492
 no ip address
 no atm ilmi-keepalive
 pvc 0/35
 pppoe-client dial-pool-number 1
!
dsl operating-mode auto
!
! Primary WAN link.
interface Dialer1
 ip address negotiated
 ip nat outside
 encapsulation ppp
 dialer pool 1
 ppp authentication pap callin
 ppp pap sent-username account password 7 pass
 ppp ipcp dns request
 ppp ipcp wins request
 ppp ipcp mask request
!
! Dialer backup logical interface.
interface Dialer3
 ip address negotiated
 ip nat outside
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 dialer pool 3
 dialer idle-timeout 60
 dialer string 5555102 modem-script Dialout
 dialer watch-group 1
!
! Remote management PC IP address.
peer default ip address 192.168.2.2
no cdp enable
!
! Need to use your own ISP account and password.
ppp pap sent-username account password 7 pass
ppp ipcp dns request
ppp ipcp wins request
ppp ipcp mask request
!
! IP NAT over Dialer interface using route-map.
ip nat inside source route-map main interface Dialer1 overload
ip nat inside source route-map secondary interface Dialer3 overload
ip classless
!
! When primary link is up again, distance 50 will override 80 if dial backup
! has not timed out. Use multiple routes because peer IP addresses are alternated
! among them when the CPE is connected.
ip route 0.0.0.0 0.0.0.0 64.161.31.254 50
ip route 0.0.0.0 0.0.0.0 66.125.91.254 50
ip route 0.0.0.0 0.0.0.0 64.174.91.254 50
ip route 0.0.0.0 0.0.0.0 63.203.35.136 80
ip route 0.0.0.0 0.0.0.0 63.203.35.137 80
ip route 0.0.0.0 0.0.0.0 63.203.35.138 80
ip route 0.0.0.0 0.0.0.0 63.203.35.139 80
ip route 0.0.0.0 0.0.0.0 63.203.35.140 80
ip route 0.0.0.0 0.0.0.0 63.203.35.141 80
ip route 0.0.0.0 0.0.0.0 Dialer1 150
no ip http server
ip pim bidir-enable
!
! PC IP address behind CPE.
access-list 101 permit ip 192.168.0.0 0.0.255.255 any
access-list 103 permit ip 192.168.0.0 0.0.255.255 any
!
! Watch multiple IP addresses because peers are alternated
! among them when the CPE is connected.
dialer watch-list 1 ip 64.161.31.254 255.255.255.255
dialer watch-list 1 ip 64.174.91.254 255.255.255.255
dialer watch-list 1 ip 64.125.91.254 255.255.255.255
!
! Dial backup will kick in if primary link is not available
! 5 minutes after CPE starts up.
dialer watch-list 1 delay route-check initial 300
dialer-list 1 protocol ip permit
!
! Direct traffic to an interface only if the dialer is assigned an IP address.
route-map main permit 10
 match ip address 101
 match interface Dialer1
!
route-map secondary permit 10
 match ip address 103
 match interface Dialer3
!
! Change console to aux function.
line con 0
 exec-timedout 0 0
 modem enable
 stopbits 1
line aux 0
 exec-timeout 0 0
 ! To enable and communicate with the external modem properly.
 script dialer Dialout
 modem InOut
 modem autoconfigure discovery
 transport input all
 stopbits 1
 speed 115200
 flowcontrol hardware
line vty 0 4
 exec-timeout 0 0
 password cisco
 login
!
scheduler max-task-time 5000
end
```

Configuring Data Line Backup and Remote Management Through the ISDN S/T Port

Cisco 880 series routers can use the ISDN S/T port for remote management. Figure 6-2 and Figure 6-3 show two typical network configurations that provide remote management access and backup for the primary WAN line. In Figure 6-2, the dial backup link goes through a customer premises equipment

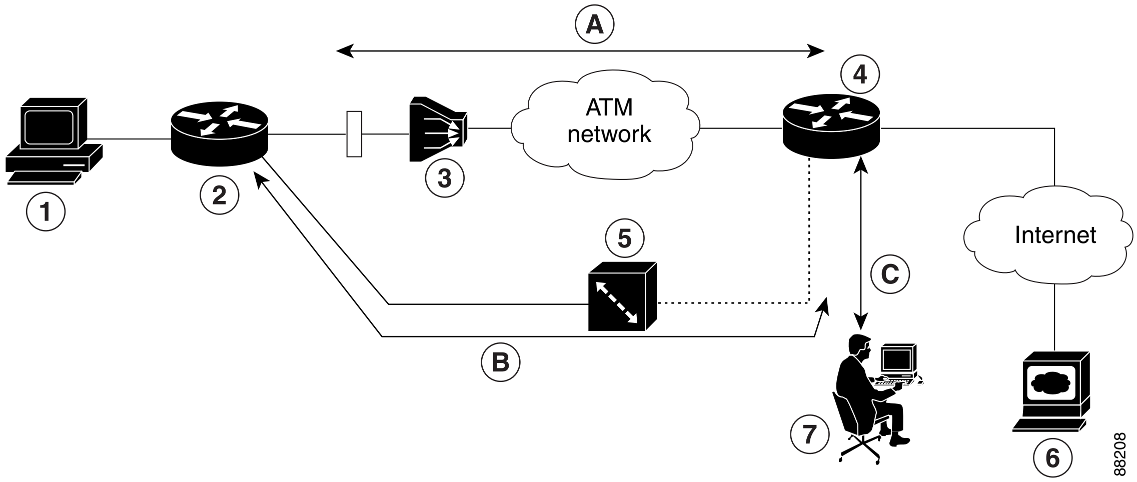
(CPE) splitter, a digital subscriber line access multiplexer (DSLAM), and a central office (CO) splitter before connecting to the ISDN switch. In Figure 6-3, the dial backup link goes directly from the router to the ISDN switch.

Figure 6-2 Data Line Backup Through CPE Splitter, DSLAM, and CO Splitter



1	Cisco 880 series router	**A**	Primary DSL interface, FE interface (Cisco 881 router)
2	DSLAM	**B**	Dial backup and remote management through the ISDN interface (ISDN S/T port); serves as a failover link when the primary line goes down
3	ATM aggregator		
4	ISDN switch		
5	ISDN	**C**	Provides administrator with remote management capability through the ISDN interface when the primary DSL link is down; serves as dial-in access to allow changes or updates to Cisco IOS configuration
6	ISDN peer router		
7	Web server		
8	Administrator	—	—

Figure 6-3 Data Line Backup Directly from Router to ISDN Switch



1	PC	**A**	Primary DSL interface
2	Cisco 880 series ISR	**B**	Dial backup and remote management through the ISDN interface (ISDN S/T port); serves as a failover link when the primary line goes down
3	DSLAM		
4	Aggregator		
5	ISDN switch	**C**	Provides administrator with remote management capability through the ISDN interface when the primary DSL link is down; serves as dial-in access to allow changes or updates to Cisco IOS configuration
6	Web server		
7	Administrator		

To configure dial backup and remote management through the ISDN S/T port of your router, perform the following procedures:

- Configuring ISDN Settings
- Configuring Aggregator and ISDN Peer Router

Configuring ISDN Settings

Note Traffic of interest must be present to activate the backup ISDN line by means of the backup interface and floating static routes methods. Traffic of interest is not needed for the dialer watch to activate the backup ISDN line.

To configure your router ISDN interface for use as a backup interface, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **isdn switch-type** *switch-type*
2. **interface** *type number*
3. **encapsulation** *encapsulation-type*

4. **dialer pool-member** *number*
5. **isdn switch-type** *switch-type*
6. **exit**
7. **interface dialer** *dialer-rotary-group-number*
8. **ip address negotiated**
9. **encapsulation** *encapsulation-type*
10. **dialer pool** *number*
11. **dialer string** *dial-string#*[**:***isdn-subaddress*]
12. **dialer-group** *group-number*
13. **exit**
14. **dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | *access-group*}

DETAILED STEPS

	Command	Purpose
Step 1	**isdn switch-type** *switch-type* **Example:** `Router(config)# isdn switch-type basic-net3`	Specifies the ISDN switch type. The example specifies a switch type used in Australia, Europe, and the United Kingdom. For details on other supported switch types, see the *Cisco IOS Dial Technologies Command Reference*.
Step 2	**interface** *type number* **Example:** `Router(config)# interface bri 0`	Enters configuration mode for the ISDN BRI.
Step 3	**encapsulation** *encapsulation-type* **Example:** `Router(config-if)# encapsulation ppp`	Sets the BRI0 interface encapsulation type.
Step 4	**dialer pool-member** *number* **Example:** `Router(config-if)# dialer pool-member 1`	Specifies the dialer pool membership.
Step 5	**isdn switch-type** *switch-type* **Example:** `Router(config-if)# isdn switch-type basic-net3`	Specifies the ISDN switch type.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits configuration interface mode and enters global configuration mode.

	Command	Purpose
Step 7	**interface dialer** *dialer-rotary-group-number* **Example:** `Router(config)# interface dialer 0`	Creates a dialer interface (numbered 0 to 255) and enters interface configuration mode.
Step 8	**ip address negotiated** **Example:** `Router(config-if)# ip address negotiated`	Specifies that the IP address for the interface is obtained through PPP/IPCP (IP Control Protocol) address negotiation. The IP address is obtained from the peer.
Step 9	**encapsulation** *encapsulation-type* **Example:** `Router(config-if)# encapsulation ppp`	Sets the encapsulation type to PPP for the interface.
Step 10	**dialer pool** *number* **Example:** `Router(config-if)# dialer pool 1`	Specifies the dialer pool to be used. In the example, the dialer pool 1 setting associates the dialer 0 interface with the BRI0 interface because the BRI0 dialer pool-member value is 1.
Step 11	**dialer string** *dial-string*#[**:***isdn-subaddress*] **Example:** `Router(config-if)# dialer string 384040`	Specifies the telephone number to be dialed.
Step 12	**dialer-group** *group-number* **Example:** `Router(config-if)# dialer group 1`	Assigns the dialer interface to a dialer group (1–10).
Step 13	**exit** **Example:** `Router(config-if)# exit`	Exits dialer 0 interface configuration mode, and enters global configuration mode.

Step 14	**dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | *access-group*}
	Example:
	`Router(config)# dialer-list 1 protocol ip permit`
		Creates a dialer list for packets of interest to be forwarded through the specified interface dialer group.
		In the example, dialer-list 1 corresponds to dialer-group 1.
		For details about this command and additional parameters that can be set, see *Cisco IOS Dial Technologies Command Reference*.

Configuring Aggregator and ISDN Peer Router

The ISDN peer router is any router that has an ISDN interface and can communicate through a public ISDN network to reach your Cisco router ISDN interface. The ISDN peer router provides Internet access for your Cisco router during the ATM network downtime.

The aggregator is typically a concentrator router where your Cisco router ATM PVC terminates. In the following configuration example, the aggregator is configured as a PPPoE server.

```
! This portion of the example configures the aggregator.
vpdn enable
no vpdn logging
!
vpdn-group 1
 accept-dialin
 protocol pppoe
 virtual-template 1
!
interface Ethernet3
 description “4700ref-1”
 ip address 40.1.1.1 255.255.255.0
 media-type 10BaseT
!
interface Ethernet4
 ip address 30.1.1.1 255.255.255.0
 media-type 10BaseT
!
interface Virtual-Template1
 ip address 22.0.0.2 255.255.255.0
 ip mtu 1492
 peer default ip address pool adsl
!
interface ATM0
 no ip address
 pvc 1/40
 encapsulation aal5snap
 protocol pppoe
!
no atm limi-keepalive
!
ip local pool adsl 22.0.0.1
ip classless
ip route 0.0.0.0 0.0.0.0 22.0.0.1 50
ip route 0.0.0.0 0.0.0.0 30.1.1.2.80

! This portion of the example configures the ISDN peer.
isdn switch-type basic-net3
!
interface Ethernet0
 ip address 30.1.1.2 255.0.0.0
!
interface BRI0
 description “to 836-dialbackup”
 no ip address
 encapsulation ppp
 dialer pool-member 1
 isdn switch-type basic-net3
!
interface Dialer0
 ip address 192.168.2.2 255.255.255.0
 encapsulation ppp
 dialer pool 1
 dialer string 384020
 dialer-group 1
 peer default ip address pool isdn
!
ip local pool isdn 192.168.2.1
ip http server
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.2.1
ip route 40.0.0.0 255.0.0.0 30.1.1.1
!
dialer-list 1 protocol ip permit!
```

Configuring Gigabit Ethernet Failover Media

Cisco 892F routers have a Gigabit Ethernet (GE) port that supports copper connections or a small-form-factor pluggable (SFP) port that supports fiber connections. Media can be configured for failover redundancy when the network goes down.

To assign primary and secondary failover media on the GE-SFP port, perform these steps, beginning in global configuration mode.

SUMMARY STEPS

1. **hostname** *name*
2. **enable secret** *password*
3. **interface gigabitethernet** *slot/port*
4. **media-type** {**sfp** | **rj45**} **auto-failove**r
5. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	**hostname** *name* **Example:** `Router(config)# hostname Router`	Specifies the name for the router.
Step 2	**enable secret** *password* **Example:** `Router(config)# enable secret cr1ny5ho`	Specifies an encrypted password to prevent unauthorized access to the router.
Step 3	**interface gigabitethernet** *slot/port* **Example:** `Router(config)# interface gigabitethernet 0/1`	Enters interface configuration mode.

Step 4	**media-type {sfp | rj45} auto-failover**
	Example:
	`Router(config-if)# media-type sfp auto-failover`
	`OR`
	`Router(config-if)# media-type rj45 auto-failover`
		Configures the port with SFP as the primary media for automatic failover from SFP to RJ-45.
		Or
		Configures the port with RJ-45 as the primary media for automatic failover from RJ-45 to SFP.

	Command	Purpose

Step 5	**exit**
	Example:
	`Router(config-if)# exit`
	`Router(config)#`
		Exits interface configuration mode and returns to global configuration mode.

Auto-Detect

The Auto-Detect feature is enabled if media-type is not configured. This feature automatically detects which media is connected and links up. If both media are connected, whichever media comes up first is linked up.

Note The Auto-Detect feature only works with 1000 Base SFPs. This feature does not detect 100 Base SFPs.

To configure the Auto-Detect feature, perform the following steps, starting in global configuration mode:

SUMMARY STEPS

1. **interface gigabitethernet** *slot/port*
2. **no media-type**
3. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	**interface gigabitethernet** *slot/port* **Example:** `Router(config)# interface gigabitethernet 0/1`	Enters interface configuration mode.

Step 2	**no media-type**
	Example:
	`Router(config-if)# no media-type`
	`GigabitEthernet0/1: Changing media to UNKNOWN.`
	`You may need to update the speed and duplex settings for this interface.`
		Enables Auto-Detect. If a 1000Base SFP is plugged in, the speed and duplex are set automatically to 1000 and full. Speed and duplex options are not available. An RJ45 connection will only work with speed as 1000 and duplex as full. If an SFP is not plugged in, all speeds and duplexes are available for the RJ45 media.
		Note The Auto-Detect feature only works with 1000Base SFPs. This feature does not detect 100Base SFPs.

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

Configuring Third-Party SFPs

Small Form-Factor Pluggables (SFPs) that are not Cisco certified are called third-party SFPs. Cisco approved means the SFPs have undergone rigorous testing with Cisco products and the SFPs are guaranteed to have 100% compatibility.

Third-party SFPs are manufactured by companies that are not on the Cisco-approved Vendor List (AVL). Currently, Cisco ISR G2 routers support only Cisco-approved SFPs. From Release 15.3(2)T, Cisco ISR G2 routers recognize third-party SFPs.

Note Cisco does not provide any kind of support for the third-party SFPs because they are not validated by Cisco.

Restrictions

- Supports only 100BASE SFPs and 1000BASE SFPs under two speed configurations:
  - 100 Mbps speed for 100BASE SFPs
  - 1000 Mbps speed for 1000BASE SFPs
- Only the following routers and modules support third-party SFPs:
  - Cisco 2921 Integrated Services Router
  - Cisco 2951 Integrated Services Router
  - Cisco 3900 Integrated Services Router
  - Cisco 3900E Series Integrated Services Routers
  - Cisco 892-F Gigabit Ethernet Security Router
  - Cisco 898-EA Gigabit Ethernet Security Router
  - EHWIC-1GE-SFP

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **service unsupported-transceiver**
4. **interface** *type slot/subslot/port number*
5. **media-type sfp**
6. **speed** *value*
7. **shutdown**
8. **no shutdown**
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**service unsupported-transceiver** **Example:** `Router(config)# service unsupported-transceiver`	Enables third-party SFP support.
Step 4	**interface** *type slot/subslot/port number* **Example:** `Router(config)# interface ethernet 0/3/0`	Selects an interface to configure.
Step 5	**media-type sfp** **Example:** `Router(config-if)# media-type sfp`	Changes media type to SFP.
Step 6	**speed** *value* **Example:** `Router(config-if)# speed 100`	Configures the speed of the interface. **Note** For 100BASE SFPs, configure the speed to 100 Mbps only. Similarly, for 1000BASE SFPs, configure the speed to 1000 Mbps only.
Step 7	**shutdown** **Example:** `Router(config-if)# shutdown`	Disables the interface, changing its state from administratively UP to administratively DOWN.
Step 8	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the interface, changing its state from administratively DOWN to administratively UP.

Step 9	**exit**
	Example:
	`Router(config-if)# exit`
	`Router(config)#`
		Exits the configuration mode and returns the global configuration mode.

Examples

This example shows how to configure a third-party SFP on a Cisco ISR G2 Series Router:

```
Router# configure terminal
Router(config-if)# service unsupported-transceiver
Router(config)# interface ethernet 0/3/0
Router(config-if)# media-type sfp
Router(config-if)# speed 100
Router(config-if)# shutdown
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# exit
```

CHAPTER 7

Configuring Ethernet Switches

This chapter gives an overview of configuration tasks for the following:

- 4-port Fast Ethernet (FE) switch on the Cisco 860, 880, and 890 integrated service routers (ISRs)
- Gigabit Ethernet (GE) switch on the Cisco 860VAE-K9
- Gigabit Ethernet (GE) switch that services the embedded wireless access point on the Cisco 860 and Cisco 880 series ISRs.

The FE switches are 10/100Base T Layer 2 Fast Ethernet switches. The GE switch is a 1000Base T Layer 2 Gigabit Ethernet switch. Traffic between different VLANs on a switch is routed through the router platform with the switched virtual interface (SVI).

Any switch port may be configured as a trunking port to connect to other Cisco Ethernet switches.

An optional power module can be added to Cisco 880 series ISRs to provide inline power to two of the FE ports for IP telephones or external access points.

This chapter contains the following sections:

Switch Port Numbering and Naming

The ports for Cisco 860, 880, and 890 ISRs are numbered as follows:

- The ports on the FE switch for the Cisco 860, 880, and 890 ISRs are numbered FE0 through FE3.
- The port on the GE switch for the 860VAE-K9 is numbered GE0.
- The port on the GE switch that services the embedded wireless access point on the Cisco 860 and Cisco 880 series ISRs is named and numbered Wlan-GigabitEthernet0.

Restrictions for the FE Switch

The following restrictions apply to the FE switch:

- Ports of an FE switch must *not* be connected to any Fast Ethernet onboard port of the router.
- On Cisco 880 series ISRs, inline power is supported only on FE switch ports FE0 and FE1. Inline power is not supported on Cisco 860 series ISRs.
- VTP pruning is not supported.
- FE switch can support up to 200 secure MAC addresses.

Information About Ethernet Switches

To configure Ethernet switches, you should understand the following concepts:

VLANs and VLAN Trunk Protocol

For information on the concepts of VLANs and VLAN Trunk Protocol (VTP), see:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt1636nm.html#wp1047027

Inline Power

Inline power is not supported on the Cisco 860 series ISRs. On the Cisco 880 series ISRs, inline power can be supplied to Cisco IP phones or external access points on FE switch ports FE0 and FE1.

A detection mechanism on the FE switch determines whether it is connected to a Cisco device. If the switch senses that there is no power on the circuit, the switch supplies the power. If there is power on the circuit, the switch does not supply it.

You can configure the switch to never supply power to the Cisco device and to disable the detection mechanism.

The FE switch also provides support for powered devices compliant with IEEE 802.3af.

Layer 2 Ethernet Switching

For information on Layer 2 Ethernet Switching, see:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt1636nm.html#wp1048478

802.1x Authentication

For information on 802.1x Authentication, see:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt1636nm.html#wp1051006

Note The **authentication** command under switch trunk interface mode is enabled for the NEAT feature. This is available with Cisco IOS Release 15.2T.

Spanning Tree Protocol

For information on Spanning Tree Protocol, see:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt1636nm.html#wp1048458

Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) runs over Layer 2 (the data link layer) on all Cisco routers, bridges, access servers, and switches. CDP allows network management applications to discover Cisco devices that are neighbors of already known devices, in particular, neighbors running lower-layer, transparent protocols. With CDP, network management applications can learn the device type and the SNMP agent address of neighboring devices. This feature enables applications to send SNMP queries to neighboring devices.

CDP runs on all LAN and WAN media that support Subnetwork Access Protocol (SNAP). Each CDP-configured device sends periodic messages to a multicast address. Each device advertises at least one address at which it can receive SNMP messages. The advertisements also contain the time-to-live, or hold-time information, which indicates the length of time a receiving device should hold CDP information before discarding it.

Switched Port Analyzer

For information on Switched Port Analyzer, see:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt1636nm.html#wp1053663

IGMP Snooping

For information on IGMP Snooping, see:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt1636nm.html#wp1053727

IGMP Version 3

The Cisco 880 series ISRs support Version 3 of IGMP snooping.

IGMPv3 provides support for source filtering, which enables a multicast receiver host to signal to a router from which groups the receiver host is to receive multicast traffic, and from which sources this traffic is expected. Enabling the IGMPv3 feature with IGMP snooping on Cisco ISRs provides Basic IGMPv3 Snooping Support (BISS). BISS provides constrained flooding of multicast traffic in the presence of IGMPv3 hosts. This support constrains traffic to approximately the same set of ports as IGMPv2 snooping does with IGMPv2 hosts. The constrained flooding only considers the destination multicast address.

Storm Control

For information on storm control, see:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt1636nm.html#wp1051018

Overview of SNMP MIBs

Simple Management Network Protocol (SNMP) development and use is centered around the MIB. An SNMP MIB is an abstract database and it is a conceptual specification for information that a management application may read and modify in a certain form. This does not imply that the information is kept in the managed system in that same form. The SNMP agent translates between the internal data structures and formats of the managed system and the external data structures and formats defined for the MIB.

The SNMP MIB is conceptually a tree structure with conceptual tables. Cisco Layer 2 Switching Interface MIB is discussed in more detail in BRIDGE-MIB for Layer 2 Ethernet Switching, page 7-4. Relative to this tree structure, the term MIB is used in two ways. One definitions of MIB is, it is actually a MIB branch, usually containing information for a single aspect of technology, such as a transmission medium or a routing protocol. A MIB used in this sense is more accurately called a MIB module, and is usually defined in a single document. The other definition of a MIB is a collection of such branches. Such a collection might comprise, for example, all the MIB modules implemented by a given agent, or the entire collection of MIB modules defined for SNMP.

A MIB is a tree where the leaves are individual items of data called objects. An object may be, for example, a counter or a protocol status. MIB objects are also sometimes called variables.

BRIDGE-MIB for Layer 2 Ethernet Switching

The Layer 2 Ethernet Switching Interface BRIDGE-MIB is supported in the Cisco 887, 880, and 890 platforms. The BRIDGE-MIB enables the user to know the Media Access Control (MAC) addresses and spanning tree information of the Ethernet switch modules. The user can query the MIB agent using the SNMP protocol and get the details of Ethernet switch modules, such as MAC addresses, of each interface and spanning protocol information.

The Bridge-MIB uses the following approaches to get the Layer 2 BRIDGE-MIB information:

- Community-string-based approach
- Context-based approach

In the community string based approach, one community string is created for each VLAN. Based on the query, the respective VLAN MIB is displayed.

To get the BRIDGE-MIB details, use the **snmp-server community public RW** command in the configuration mode.

```
Router(config)# snmp-server community public RW
```

Use the following syntax to query the SNMP BRIDGE-MIB details:

```
snmpwalk -v2c <ip address of the ISR, …>  public .1.3.6.1.2.1.17
snmpwalk -v2c <ip address of the ISR, …>  public@2 .1.3.6.1.2.1.17
snmpwalk -v2c <ip address of the ISR, …>  public@3 .1.3.6.1.2.1.17
```

Note When you create a VLAN ‘x’, the logical entity public@x is added. If you query with public community, the Layer 3 MIB is displayed. When you query with public@x, the Layer 2 MIB for VLAN ‘x’ is displayed.

In the context based approach, the SNMP context mapping commands are used to display the values for Layer 2 interfaces. Each VLAN is mapped to a context. When the user queries with a context, the MIB displays the data for that specific VLAN, which is mapped to the context. In this approach, each VLAN is manually mapped to a context.

To get the BRIDGE-MIB details, use the following commands in the configuration mode:

```
Router(config)# Routersnmp-server group public v2c context bridge-group
Router(config)# snmp-server community public RW
Router(config)# snmp-server community private RW
Router(config)# snmp-server context bridge-group
Router(config)# snmp mib community-map public context bridge-group
```

Use the following syntax to query the SNMP BRIDGE-MIB details.

```
snmpwalk -v2c <ip address of the ISR, …>  public@1 .1.3.6.1.2.1.17 ?L2-MIB
snmpwalk -v2c <ip address of the ISR, …>  private .1.3.6.1.2.1.17?L3-MIB
```

Note When you query with the public community, the Layer 2 MIB is displayed. Use a private group for Layer 3 MIB.

For more details to configure and retrieve the BRIDGE-MIB details, see:

http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094a9b.shtml#brgmib

MAC Address Notification

MAC address notification enables you to track users on a network by storing the MAC address activity on the switch. Whenever the switch learns or removes a MAC address, an SNMP notification can be generated and sent to the NMS. If you have many users coming and going from the network, you can set a trap interval time to bundle the notification traps and reduce network traffic. The MAC notification history table stores the MAC address activity for each hardware port for which the trap is enabled. MAC address notifications are generated for dynamic and secure MAC addresses; events are not generated for self addresses, multicast addresses, or other static addresses.

For more details to configure MAC address notification, see:

http://www1.cisco.com/en/US/docs/switches/lan/catalyst3550/software/release/12.2_25_see/configuration/guide/swadmin.html#wp1102213

How to Configure Ethernet Switches

See the following sections for configuration tasks for Ethernet switches:

- Configuring VLANs, page 7-6
- Configuring Layer 2 Interfaces, page 7-8
- Configuring 802.1x Authentication, page 7-8
- Configuring Spanning Tree Protocol, page 7-9
- Configuring MAC Table Manipulation, page 7-9
- Configuring Cisco Discovery Protocol, page 7-10
- Configuring the Switched Port Analyzer, page 7-10
- Configuring Power Management on the Interface, page 7-10
- Configuring IP Multicast Layer 3 Switching, page 7-10
- Configuring IGMP Snooping, page 7-10
- Configuring Per-Port Storm Control, page 7-11
- Configuring Separate Voice and Data Subnets, page 7-11
- Managing the Switch, page 7-11

Configuring VLANs

This section provides information on how to configure VLANs. The Cisco 860 series ISRs support two VLANs and the 860VAE series ISRs support five VLANs.The Cisco 880 series ISRs support eight VLANs.

- VLANs on the FE and GE Switch Ports, page 7-6
- VLANs on the GE Port and GE ESW Port of Wireless APs, page 7-7

Note Cisco 866VAE-K9 and 867VAE-K9 routers have four Fast Ethernet (FE) switching ports and one Gigabit Ethernet (GE) switching port.

VLANs on the FE and GE Switch Ports

To configure VLANs, perform these steps, beginning in configuration mode.

SUMMARY STEPS

1. **interface** *type number*
2. **shutdown**
3. **switchport access vlan** *vlan_id*
4. **no shutdown**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface** *type number* **Example:** `Router(config)# Interface fastethernet0`	Selects the Fast Ethernet port to configure.
Step 2	**shutdown** **Example:** `Router(config-if)# shutdown`	(Optional) Shuts down the interface to prevent traffic flow until configuration is complete.
Step 3	**switchport access vlan** *vlan_id* **Example:** `Router(config-if)# switchport access vlan 2`	Creates instances of additional VLANs. Allowable values of *vlan_id* are 2 to 4094, except for reserved values of 1002 to 1005.
Step 4	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the interface, changing its state from administratively down to administratively up.

Step 5	**end**
	Example:
	`Router(config-if)# end`
		Exits configuration mode.

For additional information, see the information at the following URL:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/layer2.html

VLANs on the GE Port and GE ESW Port of Wireless APs

Because the GE port is an internal interface that services only the embedded access point of the router, it cannot be configured only with the **switchport access vlan X** command, where X is other than 1. It may, however, be configured in trunk mode. This may be done by performing the following steps, beginning in global configuration mode.

SUMMARY STEPS

1. **interface** *type number*
2. **switchport mode trunk**
3. **switchport access vlan** *vlan_id*

DETAILED STEPS

	Comand or Action	Purpose
Step 1	**interface** *type number* **Example:** `Router(config)# Interface gigabitethernet0`	Selects the Gigabit Ethernet port to configure.
Step 2	**switchport mode trunk** **Example:** `Router(config-if)# switchport mode trunk`	Places the port in trunk mode.
Step 3	**switchport access vlan** *vlan_id* **Example:** `Router(config-if)# switchport access vlan 2`	(Optional) Once the port is in trunk mode, it may be assigned a VLAN number other than 1.

Configuring Layer 2 Interfaces

For information on how to configure Layer 2 interfaces, see the following URL:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/esw_cfg.html#wp1047041

The URL contains information on the following topics:

- Configuring a range of interfaces
- Defining a range macro
- Configuring Layer 2 optional interface features

Configuring 802.1x Authentication

For information on how to configure 802.1x port-based authentication, see:

http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/ht_8021x.html

The document contains information on the following topics:

- Understanding the default 802.1x configuration
- Enabling 802.1x authentication
- Configuring the switch-to-RADIUS-server comunication
- Enabling periodic reauthentication
- Changing the quiet period
- Changing the switch-to-client retransmission time
- Setting the switch-to-client frame-retransmission number
- Enabling multiple hosts
- Resetting the 802.1x configuration to default values
- Displaying 802.1x statistics and status

Configuring Spanning Tree Protocol

For information on how to configure Spanning Tree Protocol, see:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/esw_cfg.html#wp1047906

The document contains information on the following topics:

- Enabling spanning tree
- Configuring spanning tree port priority
- Configuring spanning tree port cost
- Configuring the bridge priority of a VLAN
- Configuring the Hello Time
- Configuring the forward-delay time for a VLAN
- Configuring the maximum aging time for a VLAN
- Disabling spanning tree

Configuring MAC Table Manipulation

For information on how to configure MAC table manipulation, see:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/esw_cfg.html#wp1048223

The document contains information on the following topics:

- Enabling known MAC address traffic
- Creating a static entry in the MAC address table
- Configuring the aging timer
- Verifying the aging time

Port Security

The topic of enabling known MAC address traffic deals with port security. Port security can be either static or dynamic.

Static port security allows the user to specify which devices are allowed access through a given switch port. The specification is done manually by placing allowed device MAC addresses in the MAC address table. Static port security is also known as MAC address filtering.

Dynamic port security is similar. However, instead of specifying the MAC address of the devices, the user specifies the maximum number of devices that is allowed on the port. If the maximum number specified is more than the number of MAC addresses specified manually, the switch learns the MAC address automatically, up to the maximum specified. If the maximum number specified is less than the number of MAC addresess already specified statically, an error message is produced.

The following command is used to specify static or dynamic port security.

Command	Purpose
`Router(config)#` **`mac-address-table secure`** `[`*`mac-address`* `|` **`maximum`** *`maximum addresses`*`]` **`fastethernet`** *`interface-id`* `[`**`vlan`** *`vlan id`*`]`	*mac-address* enables static port security. The **maximum** keyword enables dynamic port security.

Configuring Cisco Discovery Protocol

For information on how to configure Cisco Discovery Protocol (CDP), see:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/esw_cfg.html#wp1048365

The document contains information on the following topics:

- Enabling CDP
- Enabling CDP on an interface
- Monitoring and maintaining CDP

Configuring the Switched Port Analyzer

For information on how to configure a switched port analyzer (SPAN) session, see:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/esw_cfg.html#wp1048473

The document contains information on the following topics:

- Configuring the SPAN sources
- Configuring SPAN destinations
- Verifying SPAN sessions
- Removing sources or destinations from a SPAN session

Configuring Power Management on the Interface

For information on how to configure inline power for access points or Cisco IP phones, see:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/esw_cfg.html#wp1048551

Configuring IP Multicast Layer 3 Switching

For information on how to configure IP multicast Layer 3 switching, see:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/esw_cfg.html#wp1048610

The document contains information on the following topics:

- Enabling IP multicast routing globally
- Enabling IP protocol-independent multicast (PIM) on Layer 3 interfaces
- Verifying IP multicast Layer 3 hardware switching summary
- Verifying the IP multicast routing table

Configuring IGMP Snooping

For information on how to configure IGMP snooping, see:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/esw_cfg.html#wp1048777

The document contains information on the following topics:

- Enabling or disabling IGMP snooping
- Enabling IGMP immediate-leave processing
- Statically configuring an interface to join a group
- Configuring a multicast router port

IGMP Version 3

In support of the IGMPv3 feature in Cisco IOS Release 12.4(15)T, the **groups** and **count** keywords were added to the **show ip igmp snooping** command, and the output of the **show ip igmp snooping** command was modified to include global information about IGMP snooping groups. Use the **show ip igmp snooping** command with the **groups** keyword to display the multicast table learned by IGMP snooping for all VLANs, or the **show ip igmp snooping** command with the **groups** keyword, **vlan-id** keyword, and *vlan-id* argument to display the multicast table learned by IGMP snooping for a specific VLAN. Use the **show ip igmp snooping** command with the **groups** and **count** keywords to display the number of multicast groups learned by IGMP snooping.

Configuring Per-Port Storm Control

For information on how to configure per-port storm control, see:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/esw_cfg.html#wp1049009

The document contains information on the following topics:

- Enabling per-port storm-control
- Disabling per-port storm-control

Configuring Separate Voice and Data Subnets

For information on how to configure separate voice and data subnets, see:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/esw_cfg.html#wp1049866

Managing the Switch

For information on management of the switch, see:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/esw_cfg.html#wp1049978

The document contains information on the following topics:

- Adding Trap Managers
- Configuring IP Information
- Enabling Switch Port Analyzer
- Managing the ARP Table
- Managing the MAC Address Tables
- Removing Dynamic Addresses
- Adding Secure Addresses

- Configuring Static Addresses
- Clearing all MAC Address Tables

CHAPTER 8

Configuring Voice Functionality

This chapter provides information about configuring voice functionality on the Cisco 880 Series Integrated Services Routers (ISRs). The following ISRs have voice gateway capability:

- C881SRST and C888SRST: 4 FXS ports and 1 voice backup port
  - The C881SRST ISR has an FXO voice backup port.
  - The C888SRST ISR has a BRI voice backup port.
- C881-V has 4FXS ports, 2 BRI ports, and 1 backup FXO port
- C887VA-V and C887VA-V-W has 4FXS ports and 2 BRI ports.

This chapter contains the following topics:

Voice Ports

Analog voice ports (Foreign Exchange Station (FXS) ports) connect routers in packet-based networks to 2-wire or 4-wire analog circuits in telephony networks. Two-wire circuits connect to analog telephone or fax devices, and four-wire circuits connect to PBXs.

Digital voice ports are ISDN basic rate interface (BRI) ports.

Analog and Digital Voice Port Assignments

Analog and digital voice port assignments vary by model number. Table 8-1 lists the Cisco 880 series ISRs and their voice port assignments.

Table 8-1 Voice Port Assignments for Cisco 880 series ISRs

Model Number	Digital (BRI) Port Numbers	Analog (FXS) Port Numbers	Voice Backup Port Number
C881SRST	—	0–3	4 (FXO port)
C888SRST	—	0–3	4 (BRI port)
C881-V	2	4	1 (FXO port)
C887VA-V	2	4	—
C887VA-V-W	2	4	—

Voice Port Configuration

To configure analog and digital voice ports, see the following documents:

- *Configuring Analog Voice Ports*
- *Basic ISDN Voice Interface Configuration*

Call Control Protocols

The Cisco 880 Series ISR voice gateway models support the following call control protocols:

- SIP, page 8-2
- MGCP, page 8-3
- H.323, page 8-3

SIP

Session Initiation Protocol (SIP) is a peer-to-peer, multimedia signaling protocol developed in the IETF (IETF RFC 2543). Session Initiation Protocol is ASCII-based. It resembles HTTP, and it reuses existing IP protocols (such as DNS and SDP) to provide media setup and teardown. See the *Cisco IOS SIP Configuration Guide, Release 4T* for more information.

For router configuration information under SIP, see the *Basic SIP Configuration* chapter of the *Cisco IOS SIP Configuration Guide, Release 4T.*

Cisco 880 Series ISR voice gateways provide voice security through SIP enhancements within the Cisco IOS Firewall. SIP inspect functionality (SIP packet inspection and detection of pin-hole openings) is provided, as well as protocol conformance and application security. The user is given more granular control on the policies and security checks applied to SIP traffic, and capability to filter out unwanted messages. For more information, see "Cisco IOS Firewall: SIP Enhancements: ALG and AIC" at http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_sip_alg_aic.html.

MGCP

Media Gateway Control Protocol (MGCP) RFC 2705 defines a centralized architecture for creating multimedia applications, including Voice over IP (VoIP). See the *Cisco IOS MGCP and Related Protocols Configuration Guide* for more information.

Cisco 880 series voice gateway ISRs are configured primarily as residential gateways (RGWs) under MGCP. For residential gateway configuration information, see the *Configuring an RGW* section of the *Basic MGCP Configuration* chapter of the *Cisco IOS MGCP and Related Protocols Configuration Guide*.

H.323

International Telecommunications Union Recommendation H.323 defines a distributed architecture for creating multimedia applications, including Voice over IP. See the *Cisco IOS H.323 Configuration Guide, Release 12.4T* for more information about H.323.

For router configuration information, see the *Configuring H.323 Gateways* chapter of the *Cisco IOS H.323 Configuration Guide, Release 12.4T*.

Dial Peer Configuration

Configuring dial peers is the key to implementing dial plans and providing voice services over an IP packet network. Dial peers are used to identify call source and destination endpoints and to define the characteristics applied to each call leg in the call connection. For router configuration information, see *Dial Peer Configuration on Voice Gateway Routers*.

Other Voice Features

The Cisco 880 series voice gateway ISRs support the following voice features:

- Real-Time Transport Protocols, page 8-3
- Dual Tone Multi Frequency Relay, page 8-4
- CODECs, page 8-4
- SCCP-Controlled Analog Ports with Supplementary Features, page 8-4

Real-Time Transport Protocols

Real-Time Transport Protocol (RTP) provides end-to-end network transport functions for applications that transmit real-time data.

Cisco Real-Time Transport Protocol (cRTP) uses the RTP protocol to forward Cisco-proprietary payload types.

Secure Real-Time Transport Protocol (SRTP) defines an RTP profile providing encryption, authentication, and replay protection.

RTP is used primarily with DTMF relay and is configured under dial peer configuration. For information on configuring RTP payload types, see the *Dual-Tone Multifrequency Relay* section of *Dial Peer Configuration on Voice Gateway Routers*.

For information on configuring SRTP on SIP-controlled platforms, see the *Configuring SIP Support for SRTP* chapter of the *Cisco IOS SIP Configuration Guide, Release 4T*.

For configuring RTP on MGCP-controlled platforms, see the *Configuring an RGW* section of the *Basic MGCP Configuration* chapter of the *Cisco IOS MGCP and Related Protocols Configuration Guide*.

Dual Tone Multi Frequency Relay

Using Dial Tone Multi Frequency (DTMF) Relay the local VoIP gateway listens for DTMF digits and sends the digits uncompressed as either RTP packets or H.245 packets to the remote VoIP gateway. The remote VoIP gateway regenerates the DTMF digits. This methodology prevents digit loss due to compression. For information on configuring DTMF Relay, see the *Dual-Tone Multifrequency Relay* section of *Dial Peer Configuration on Voice Gateway Routers*.

For information on configuring DTMF that is specific to call control protocols, see the following:

- *Configuring SIP DTMF Features*
- *Configuring DTMF Relay* (H.323)
- *Configuring Global MGCP Parameters*

CODECs

The following CODECs are supported by the Cisco 880 series voice gateway routers.

- G.711 (a-law and mu-law)
- G.726
- G.729, G.729A, G.729B, G.729AB

For information on CODECs, see the following:

- *Dial Peer Configuration Examples* appendix of *Dial Peer Configuration on Voice Gateway Routers.*
- *Cisco IOS SIP Configuration Guide, Release 4T*
- *Cisco IOS H.323 Configuration Guide*
- *Configuring Global MGCP Parameters*

SCCP-Controlled Analog Ports with Supplementary Features

Cisco 880 series voice gateway ISRs support the Cisco Skinny Client Control Protocol (SCCP) that supplies supplementary features on analog voice ports that are controlled by Cisco Unified Communications Manager or by a Cisco Unified Communications Manager Express system. Supported features include:

- Audible message waiting indication
- Call forwarding options
- Call park/pickup options
- Call transfer

- Call waiting
- Caller ID
- 3-party conference calls
- Redial
- Speed dial options

For more information on the features supported and their configuration, see *SCCP Controlled Analog (FXS) Ports with Supplementary Features in Cisco IOS Gateways*.

Fax Services

The Cisco 880 series voice gateway ISRs support the following fax services:

- Fax Pass-Through, page 8-5
- Cisco Fax Relay, page 8-5
- T.37 Store-and-Forward Fax, page 8-5
- T.38 Fax Relay, page 8-5

Fax Pass-Through

Fax Pass-Through is the simplest way of transmitting faxes over IP, although it is not as reliable as Cisco Fax Relay. See the *Configuring Fax Pass-Through* chapter of the *Cisco IOS Fax, Modem, and Text Services over IP Configuration Guide* for more information.

Cisco Fax Relay

Cisco Fax Relay is a Cisco proprietary fax method that is turned on by default. Cisco Fax Relay allows the relay of a T.30 modulated signal across IP gateways in real-time on H.323 or SIP networks. See the *Configuring Cisco Fax Relay* chapter of the *Cisco IOS Fax, Modem, and Text Services over IP Configuration Guide* for more information.

T.37 Store-and-Forward Fax

The T.37 Store-and-Forward Fax mechanism allows a gateway to store and forward fax messages on H.323 or SIP networks. See the *Configuring T.37 Store-and-Forward Fax* chapter of the *Cisco IOS Fax, Modem, and Text Services over IP Configuration Guide* for more information.

T.38 Fax Relay

The T.38 Fax Relay provides an ITU-standard mechanism for real-time relay of fax signals. Gateway-controlled T.38 Fax Relay is available on MGCP networks. See the *Configuring T.38 Fax Relay* chapter of the *Cisco IOS Fax, Modem, and Text Services over IP Configuration Guide* for more information.

Unified Survival Remote Site Telephony

Cisco 880 Series voice gateway ISRs with Unified Survival Remote Site Telephony (SRST) include the following:

- Cisco C881SRST
- Cisco C888SRST

Unified SRST automatically detects a failure in the network and initializes the process of auto configuring the router. Unified SRST provides redundancy for the IP and FXS phones to ensure that the telephone system remains operational.

All the IP phones and analog phones connected to a telecommuter site are controlled by the headquarters office call control system, which uses Cisco Unified Communications Manager. During a WAN failure, the telecommuter router allows all the phones to reregister to the headquarter in SRST mode, allowing all inbound and outbound dialing to be routed off to the PSTN (on a backup Foreign Exchange Office (FXO) or BRI port). Upon restoration of WAN connectivity, the system automatically returns communication to the primary Cisco Unified Communications Manager cluster.

Direct Inward Dialing (DID) is supported on the Cisco 880 series SRST voice gateway ISRs.

For general Unified SRST information, see the *Cisco Unified SRST System Administrator Guide*. Cisco Unified SRST is described in the *Overview* chapter.

- For information on how the H.323 and MGCP call control protocols relate to SRST, see the following sections of the *Overview* chapter in the *Cisco Unified SRST System Administrator Guide:*
  - For H.323, see *Cisco Unified SRST Description*
  - For MGCP, see *MGCP Gateways and SRST*
- Configurations of major SRST features are provided in the following chapters of the *Cisco Unified SRST System Administrator Guide*:
  - *Setting Up the Network*
  - *Setting Up Cisco Unified IP Phones*
  - *Setting Up Call Handling*
  - *Configuring Additional Call Features*
  - *Setting Up Secure SRST*
  - *Integrating Voice Mail with Cisco Unified SRST*

For SIP-specific SRST information, see the *Cisco Unified SIP SRST System Administrator Guide*. To configure SIP SRST features, see the *4.1 Features* chapter.

Verification of Voice Configuration

Use the following procedures to verify voice port configurations:

- *Cisco IOS Voice Port Configuration Guide, Verifying Analog and Digital Voice Port Configurations*
- *Cisco IOS Voice Port Configuration Guide, Verify BRI Interfaces*

To verify, monitor, and maintain SRST, see *Monitoring and Maintaining Cisco Unified SRST.*

CHAPTER 9

Basic Wireless Device Configuration

This module describes how to configure the autonomous wireless device on the following Cisco Integrated Services Routers (ISRs):

- Cisco 860 Series
- Cisco 880 Series
- Cisco 890 Series

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 9-8 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, page 9-1
- Configuring Wireless Settings, page 9-4
- Configuring the Access Point in Hot Standby Mode, page 9-8 (Optional)
- Upgrading to Cisco Unified Software, page 9-8
- Related Documentation, page 9-11

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 command-line interface (CLI).

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	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.
		Note 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 shut** **Example:** `Router(config-if)# no shut`	Specifies that the internal interface connection will remain open.
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 860 Series, Cisco 880 Series, and Cisco 890 Series ISRs.

	Command or Action	Purpose

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 interface configuration mode and returns to global 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. After entering this command, you utomatically skip to the **dot11 radio** level in the Cisco IOS software.

Closing the Session

To close the session between the wireless device and the router's console, perform the following steps.

Wireless Device

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

Router

2. **disconnect**
3. Press **Enter** twice.

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 9-1.

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

- Cisco IOS Command Line Interface, page 9-4—Autonomous software
- Cisco Express Setup, page 9-4—Unified Software

Note To upgrade to Unified mode from the Autonomous mode, see the "Upgrading to Cisco Unified Software" section on page 9-8 for upgrade instructions.

After upgrading to Cisco Unified Wireless software, use the web-browser tool to configure the device: 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 Unified 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 user name.

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://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 and perform these tasks:

- Configuring the Radio, page 9-5
- Configuring Wireless Security Settings, page 9-5
- Configuring Wireless Quality of Service, page 9-8 (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 Chapter 10, “Configuring Radio Settings”.

Configuring Wireless Security Settings

- Configuring Authentication, page 9-5
- Configuring WEP and Cipher Suites, page 9-6
- Configuring Wireless VLANs, page 9-6

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.

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 9-7. 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.

Read 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 the security setting for an SSID conflicts with the settings for another SSID, delete one or more SSIDs to eliminate the conflict.

Security Types

Table 9-1 describes the four security types that you can assign to an SSID.

Table 9-1 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.	None.
Static WEP key	This option is more secure than no security. However, static WEP keys are vulnerable to attack. If you configure this setting, you should consider limiting association to the wireless device based on MAC address, see *Cipher 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. See *Using the Access Point as a Local Authenticator* for instructions: 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.
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 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. User 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 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 off line 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 9-9
- Performing the Upgrade, page 9-10
- Downgrading the Software on the Access Point, page 9-11
- Recovering Software on the Access Point, page 9-11

Software Prerequisites

- Cisco 890 Series ISRs with embedded access points can be upgraded from autonomous software to Cisco Unified software, if the router is running the IP Base feature set and Cisco IOS 12.4(22)YB software.
- Cisco 880 Series ISRs with embedded access points can be upgraded from autonomous software to Cisco Unified software, if the router is running the advipservices feature set and Cisco IOS 12.4(20)T software.
- To use the embedded access point in a Cisco Unified Architecture, the Cisco Wireless LAN Configuration (WLC) must be running version 5.1 or later.

Preparing for the Upgrade

Perform the tasks in the following sections to prepare for the upgrade:

- Secure an IP Address on the Access Point, page 9-9
- Confirm that the Mode Setting is Enabled, page 9-9

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 boot up. The host router provides the access point DHCP server functionality through the DHCP pool. The access point then communicates with the WLC and setup option 43 for the controller IP address in the DHCP pool configuration. The following example shows 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, perform the following 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 sample output for the command:

```
Autonomous-AP# show boot
BOOT path-list:      flash:ap801-k9w7-mx.124-10b.JA3/ap801-k9w7-mx.124-10b.JA3
Config file:         flash:/config.txt
Private Config file: flash:/private-config
Enable Break:        yes
Manual Boot:         yes
HELPER path-list:
NVRAM/Config file
buffer size:   32768
Mode Button:    on
```

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*), use the **service-module wlan-ap 0 bootimage unified** command, in global configuration mode.

```
Router# conf 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 successfully, check whether the software license is still eligible.

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:/ap801-rcvk9w8-mx/ap801-rcvk9w8-mx
```

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

See the "Cisco Express Setup" section on page 9-4 for details about using the GUI configuration page to set up the wireless device settings.

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 seems 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.
- 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 will 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.

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 global configuration mode. To reload the access point with the autonomous software image, use the **service-module wlan-ap 0 reload** command.

Recovering Software on the Access Point

To recover the image on the access point, use the **service-module wlan-ap0 reset bootloader** command in global configuration 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.

Related Documentation

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

- Autonomous Cisco Documentation—Table 9-2
- Cisco Unified Documentation—Table 9-3

Table 9-2 Autonomous Cisco Documentation

Network Design	**Links**
Wireless Overview	Chapter 2, "Wireless Device Overview"
Configuration	**Links**
Configuring the Radio	Chapter 10, "Configuring Radio Settings"
Security	**Links**
Authentication Types for Wireless Devices	This document describes the authentication types that are configured on the access point. http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html
RADIUS and TACACS+ Servers in a Wireless Environment	This document describes how to enable and configure the RADIUS and TACACS+ and provides detailed accounting information and flexible administrative control over authentication and authorization processes. RADIUS and TACACS+ are facilitated through AAA[1] and can be enabled only through AAA commands. http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityRadiusTacacs_1.html
Using the Access Point as a Local Authenticator	This document 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. http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html
Cipher Suites and WEP	This document describes how to configure the cipher suites required for using WPA and CCKM[2]; WEP; and WEP features including AES[3], MIC[4], TKIP, and broadcast key rotation. http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityCipherSuitesWEP.html
Hot Standby Access Points	This document describes how to configure your wireless device as a hot standby unit. http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/RolesHotStandby.html
Configuring Wireless VLANs	This document describes how to configure an access point to operate with the VLANs set up on a wired LAN. http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/wireless_vlans.html
Service Set Identifiers	In the role of an access point, a wireless device can support up to 16 SSIDs. This document describes how to configure and manage SSIDs on the wireless device. http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/ServiceSetID.html
Administering	**Links**

Table 9-2 Autonomous Cisco Documentation (continued)

Network Design	Links
Administering the Access Point	Chapter 12, "Administering the Wireless Device"
Quality of Service	This document describes how to configure QoS 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. http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/QualityOfService.html
Regulatory Domains and Channels	This document lists the radio channels supported by Cisco access products in the regulatory domains of the world. http://www.cisco.com/en/US/customer/docs/routers/access/wireless/software/guide/RadioChannelFrequencies.html
System Message Logging	This document describes how to configure system message logging on your wireless device. http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SysMsgLogging.html

[1] AAA = Authentication, Authorization, and Accounting.

[2] CCKM = Cisco Centralized Key Management.

[3] AES = Advanced Encryption Standard.

[4] MIC = Message Integrity Check.

Table 9-3 Cisco Unified 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
Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges, versions 12.4(10b) JA and 12.3(8) JEC	http://www.cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/command/reference/cr2410b.html
Cisco Aironet 1240AG Access Point Support Documentation	http://www.cisco.com/en/US/docs/wireless/access_point/1240/quick/guide/ap1240qs.html
Cisco 4400 Series Wireless LAN Controllers Support Documentation	http://www.cisco.com/en/US/products/ps6366/tsd_products_support_series_home.html

Configuring Radio Settings

This section 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.

	Command or Action	Purpose

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 10-2.

Note Fast Ethernet tracking does not support the repeater mode.

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

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

MAC-Address Tracking

You can configure the radio whose role is root access point to 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 1 shows potential data rated based on MCS, guard interval, and channel width.

Table 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 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. **onfigure 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 10-14 for more information.

	Command or Action	Purpose
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.

	Command or Action	Purpose

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 10-20 for instructions on setting up protected ports.

To enable and disable PSPF using CLI commands on the wireless device, you use bridge groups. You can find a detailed explanation of bridge groups and instructions for implementing them in this document:

- *Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.2*. Click this link to browse to the Configuring Transparent Bridging chapter:

  http://www.cisco.com/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*. Click this link to browse to that guide:

http://www.cisco.com/en/US/docs/switches/lan/catalyst3550/software/release/12.1_12c_ea1/configuration/guide/3550scg.html

Configuring the Beacon Period and the DTIM

The beacon period is the amount of time between access point beacons in kilomicroseconds (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**.

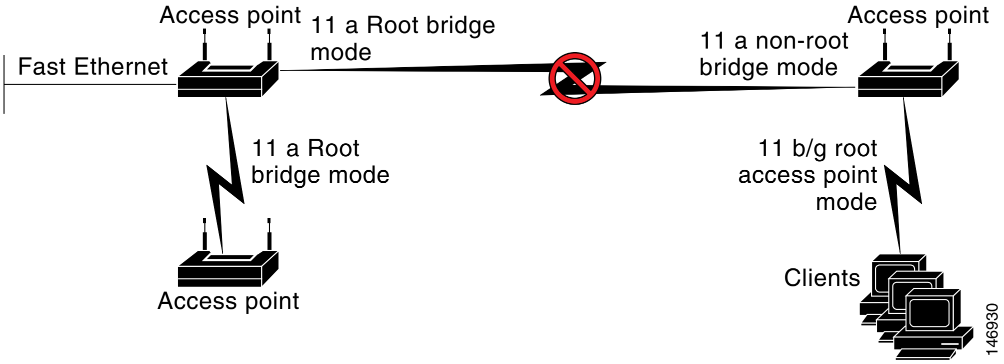
The Stream page appears.

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

Figure 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*.

CHAPTER 11

Configuring WLAN

This section describes the configuration tasks for Cisco C866VAE-W-E-K9, C867VAE-W-A-K9, C867VAE-W-E-K9, and C867VAE-POE-W-A-K9 routers.

This chapter contains the following sections:

Configuring WLAN Using the Web-based Interface

Use the web-based interface to display wireless LAN (WLAN) information and configure settings. For information about the CLI-based WLAN interface, see Configuring WLAN Using the CLI-based Interface, page 11-8.

See the following sections:

Connecting to the Web-based WLAN Interface

To connect to the web-based WLAN interface, open the following address in a web browser: http://10.10.10.2

Log in using the default credentials:

User name: **admin**

Password: **admin**

Note When using the default WLAN credentials, the user is prompted to change the password when logging in for the first time.

Address for Accessing Web-based Interface

You can change the address for accessing the web-based interface. See Configuring Access to the Web-based Interface, page 11-2.

DHCP Server Configuration

By default, the DHCP server is not configured. Configure DHCP parameters using the Cisco IOS CLI on VLAN 1.

Subnet

Connect to the interface from a device within the LAN containing the router. The device must be within the subnet configured for accessing the router. The default subnet mask is 255.255.255.0.

Displaying Device Information

In the left pane, click **Device Info > Summary** to open the Device Info page, displaying the following device information:

- Hardware and driver information for upgrading drivers or troubleshooting

Displaying Connection Statistics

In the left pane, click **Device Info > Statistics** to open the Statistics - WLAN page, displaying statistics on packets received and packets transmitted. The page is automatically refreshed.

Configuring Access to the Web-based Interface

In the left pane, click **Device Info > Network Interface** to open the Network Interface Setup page for configuring access to the web-based interface.

The page shows the IP address and subnet mask used to access the web-based interface. You can enter a new IP address and subnet mask for accessing the web-based interface. The default values are:

IP: **10.10.10.2**

Subnet Mask: **255.255.255.248**

Note Enter IPv4 values only. IPv6 is not supported.

Note Changing the IP address to a different subnet requires changing VLAN 1 to be in the same subnet also.

Note You can access the web-based interface only from a device within the same subnet.

Configuring Basic Wireless Settings

In the left pane, click **Wireless > Basic** to open the Wireless - Basic page, providing configuration options for the wireless LAN (WLAN).

Main SSID

The options in the top portion of the Wireless - Basic page apply to the main service set identification (SSID):

- Enable Wireless—Enables/disables the WLAN feature.
- Hide Access Point—Hiding the SSID provides a small measure of security in helping to prevent unauthorized users from accessing the network. When this feature is enabled, the WLAN access point SSID is not broadcast, making wireless snooping more difficult.
- Clients Isolation—Prevents a wireless client connected to a specific SSID from communicating with other wireless clients connected to the same SSID.
- Disable WMM Advertise—Disables the WiFi Multimedia (WMM) feature. The WMM feature prioritizes media traffic to improve media transmission.
- Enable Wireless Multicast Forwarding (WMF)—Enables the Wireless Multicast Forwarding (WMF) feature.
- SSID—Main SSID used for accessing the WLAN. Devices connected to the WLAN using the same SSID operate within the same domain. The main SSID can be disabled only by disabling WLAN completely.
- BSSID—MAC address for the main SSID. Each enabled SSID has a separate BSSID.
- Max Clients—Configures the maximum number of clients that can connect to the main SSID.
  Default value: 16
  Recommended maximum: 16
  Theoretical maximum: 128

Guest SSIDs

A table at the bottom of the Wireless - Basic page shows the guest SSIDs for connecting guest devices to the WLAN. For each guest SSID, you can configure options similar to those for the main SSID.

Default SSID Values

The following are the default SSID values:

- Main SSID: Cisco860
- Guest SSID 1: Cisco860_Guest1
- Guest SSID 2: Cisco860_Guest2
- Guest SSID 3: Cisco860_Guest3

Note By default, the main SSID is enabled and guest SSIDs are disabled.

Configuring Security

In the left pane, click **Wireless > Security** to open the Wireless - Security page, providing security settings for each access point.

Complete the following steps to configure security settings for an access point:

Step 1 In the Select SSID drop-down list, select the SSID to configure.

Step 2 Using the drop-down lists, select network authentication options for the SSID. Selecting an authentication type displays additional options specific to the authentication type.

Note By default, the network authentication is open and WEP encryption is disabled for each SSID.

Step 3 Click **Apply/Save**.

Configuring MAC Filtering

In the left pane, click **Wireless > MAC Filter** to open the Wireless - MAC Filter page, enabling you to restrict access to specific SSIDs according to device MAC addresses.

For each SSID, you can specify MAC addresses to allow or MAC addresses to deny. By default, the MAC restriction feature is disabled for all SSIDs.

Complete the following steps to configure MAC filtering for an SSID:

Step 1 In the Select SSID drop-down list, select the SSID to configure.

Step 2 To add a MAC address to the list, click **Add** and enter the address.

Step 3 To remove a MAC address from the list, select the “Remove” check box for the address and click **Remove**.

Step 4 Select a MAC restriction mode:

- Disabled—The feature is disabled.
- Allow—Allow devices with the specified MAC addresses to connect.
- Deny—Do not allow devices with the specified MAC addresses to connect.

Configuring Advanced Wireless Settings

In the left pane, click **Wireless > Advanced** to open the Wireless - Advanced page for configuring the advanced wireless LAN (WLAN) features described in Table 11-1.

Table 11-1 Advanced WLAN

Option	Description
Band	Frequency band. This is preset to 2.4 GHz.
Channel	Radio channels. By default, the router sets the channel automatically. You can select a specific channel. The channel options depend on the geographic region.
Auto Channel Timer (min)	(Enabled when Channel is set to Auto) Minutes to wait before scanning again to determine the best channel. Range: 1 to 35791394 minutes.
802.11n/EWC	Enables/disables 802.11n support.
802.11n Rate	(802.11n/EWC must be set to Auto) Configures the rate for 802.11n.
802.11n Protection	(802.11n/EWC must be set to Auto) Configures RTS/CTS protection.
Support 802.11n Client Only	(802.11n/EWC must be set to Auto) Restricts support to 802.11n only.
RIFS Advertisement	(802.11n/EWC must be set to Auto) Enables/disables Reduced Inter-Frame Space (RIFS) Advertisement.
RX Chain Power Save	(802.11n/EWC must be set to Auto) Enables/disables the power save mode.
RX Chain Power Save Quiet Time	(802.11n/EWC must be set to Auto and RX Chain Power Save must be set to Enable) Time interval (seconds) to wait before going into the power save mode. Range: 0 to 2147483647 seconds.

Option	Description
RX Chain Power Save PPS	(802.11n/EWC must be set to Auto and RX Chain Power Save must be set to Enable) Packets per second (PPS) threshold. When the PPS is below the threshold, the router enters power save mode after the number of seconds configured in the "RX Chain Power Save Quiet Time" field. Range: 0 to 2147483647 packets per second.
54g Rate	(802.11n/EWC must be set to Disabled or 802.11n Rate must be set to "Use 54g Rate") Configures the 54g rate.
Multicast Rate	Transmit/Receive rate for multicast packets. **Note** If 802.11n/EWC is Disabled and "54g Mode" is set to "802.11b Only," then the options will change.
Basic Rate	Data rate that wireless clients should support.
Fragmentation Threshold	Maximum packet size (bytes) before data is fragmented. Range: 256 to 2346 bytes.
RTS Threshold	RTS threshold value that will trigger the CTS protection mechanism. If an access point transmits a packet larger than the threshold, this will trigger the CTS protection mode. Range: 0 to 2347 bytes.
DTIM Interval	Delivery Traffic Indication Message (DTIM) interval information is included in beacon frames to inform clients of when next to expect buffered data from AP. The interval is specified as number of beacons. For example, if DTIM interval is set to 2, the client will wake-up/check for buffered data on AP at every second beacon. Range: 1 to 255 beacons.
Beacon Interval	Length of time between beacon transmissions. Range: 1 to 65535 milliseconds.
Global Max Clients	Upper limit for the maximum number of clients that can connect to an AP. The "Max Clients" setting for each SSID cannot exceed this limit. Range: 1 to 128 Default value: 16 Recommended maximum: 16 Theoretical maximum: 128
Transmit Power	Configures the transmit power level.
WMM (Wi-Fi Multimedia)	Enables/disables the WMM feature, a quality of service (QoS) feature of 802.11.
WMM No Acknowledgement	(WMM (Wi-Fi Multimedia) must be set to Enabled or Auto) Enables/disables the WMM No Acknowledgement feature.

Option	Description
WMM APSD	(WMM (Wi-Fi Multimedia) must be set to Enabled or Auto) Enables/disables the WMM Automatic Power Save Delivery feature. **Note** When WMM is in Auto mode, WMM APSD must be set to Enabled to enable a client to use Power Save Mode. When WMM is in Enabled mode, the client can use Power Save Mode regardless of whether WMM APSD is Enabled or Disabled.
54g Mode	(802.11n/EWC must be set to Disabled) Configures 54g mode.
54g Protection	(802.11n/EWC must be set to Disabled) Setting this field to Auto enables the RTS/CTS Protection mechanism.
Preamble Type	(802.11n/EWC must be set to Disabled. 54g Mode must be set to either “54g Auto” or “802.11b only”.) Defines the length of the cyclic redundancy code (CRC) block used for AP-to-WLAN client communication.

Station Info

In the left pane, click **Wireless > Station Info** to open the Wireless - Authenticated Stations page, displaying clients that have been authenticated for wireless LAN (WLAN) and the status of each client.

Configuring the Password for Connecting to the Web-based Interface

In the left pane, click **Management** to open the Access Control - Passwords page for configuring the administrative password.

The user name must be **admin**. You can follow the instructions on this page to change the password. The default password is **admin**.

Note The administrative account has unrestricted permission to configure the router.

Note To restore WLAN config to the default, delete the wlconfig.txt file from the flash memory, using the Cisco IOS CLI.

Saving the Wireless LAN Configuration to a File

In the left pane, click **Configuration > Backup** to save a configuration file for the wireless configuration. The file is saved locally on the workstation being used to access the GUI. For information about loading the saved configuration from the local file, see Loading a Wireless LAN Configuration File, page 11-8.

Loading a Wireless LAN Configuration File

In the left pane, click **Configuration > Update** to load a configuration file for the wireless LAN configuration from the workstation being used to access the GUI.

Caution Loading a configuration file restarts the router, interrupting any current connections.

For information about saving a configuration file locally, see Saving the Wireless LAN Configuration to a File, page 11-7.

Note A configuration file can be used to load a specific configuration onto several different routers.

Restoring the Default Configuration

In the left pane, click **Configuration > Restore Default** to restore the wireless LAN configuration to default.

Caution Restoring the default configuration restarts the router, interrupting any current connections.

Configuring WLAN Using the CLI-based Interface

Use the CLI-based interface to display wireless LAN (WLAN) information and configure settings. For information about the web-based WLAN interface, see Configuring WLAN Using the Web-based Interface, page 11-1.

See the following sections:

- About the WLAN CLI Interface, page 11-10
- Connecting to the WLAN CLI Interface, page 11-11
- Exiting from the WLAN CLI Interface, page 11-11
- Setting the IP Address for the Web-based Interface, page 11-12
- Enabling and Disabling WLAN, page 11-13
- Configuring the Main SSID, page 11-13
- Configuring Guest SSIDs, page 11-14
- Enabling and Disabling Guest SSIDs, page 11-15
- Hiding an Access Point, page 11-15
- Enabling and Disabling Client Isolation, page 11-16
- Enabling and Disabling WMM Advertise, page 11-17
- Enabling and Disabling Wireless Multicast Forwarding (WMF), page 11-18
- Configuring the Global Maximum Number of Clients, page 11-19
- Configuring the Maximum Number of Clients for an SSID, page 11-20

About the WLAN CLI Interface

The WLAN CLI interface is similar to the CLI interface for IOS.

Modes

When you enter the CLI interface, the prompt appears as:

```
ap#
```

Configuration Mode

Similarly to Cisco IOS, the prompt indicates the command mode. For example, using the **configure terminal** command to enter global configuration mode changes the prompt to:

```
ap(config)#
```

Exiting a Mode

To exit from a specific mode, use the **exit** command. For example:

```
ap(config)# exit
ap#
```

Displaying Command Information

Entering a question mark (**?**) displays information about available command options. This feature provides a simple access to information about commands and relevant command options.

Example 1

In interface configuration mode, entering **?** at the prompt displays the commands available in that mode:

```
ap(config-if)# ?
        exit                      Exit from config-if mode
        ip                        Interface Internet Protocol config commands
        no                        Negate a command or set its defaults
        shutdown                  Shutdown the interface
```

Example 2

In SSID configuration mode, entering **encryption mode wep ?** displays the options available for configuring WEP encryption mode with the **encryption mode wep** command, as follows:

```
ap(config-ssid)# encryption mode wep ?
        current-key               Network Key to use
        encryption-strength       Encryption strength
        key                       Set encryption keys
        <cr>
```

Three arguments (*current-key*, *encryption-strength*, and *key*) may be entered for the command. The <cr> option indicates that **encryption mode wep** is valid by itself without additional options. In this example, entering the command without additional arguments enables WEP encryption.

Connecting to the WLAN CLI Interface

To connect to the WLAN CLI interface, complete the following steps.

Step 1 From the Cisco IOS command line, create a loopback interface, specifying any desired IP address. For information about creating a loopback interface in Cisco IOS, see the *Cisco IOS Master Commands List*: http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html

Step 2 Connect by Telnet to the IP address specified for the loopback interface and port 2002.

Step 3 Log in when prompted.

The router displays the WLAN CLI interface prompt:

```
ap#
```

Note The default login credentials are:
User name: **admin**
Password: **admin**

When logging in for the first time, the router prompts you to change the default password.

Example of Configuring a Loopback Interface

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface loopback 0
Router(config-if)# ip address 1.1.1.1 255.255.255.0
Router(config-if)# end
```

Example of the Accessing WLAN CLI Using Telnet Through the Loopback Interface

```
Router# telnet 1.1.1.1 2002
Trying 1.1.1.1, 2002 ... Open

Connecting to AP console, enter Ctrl-^ followed by x,
then "disconnect" to return to router prompt

ap#
```

Exiting from the WLAN CLI Interface

To exit from the WLAN CLI and return to the Cisco IOS CLI prompt, press **CTRL-SHIFT-6**, followed by **x**, then “**disconnect**”.

Setting the IP Address for the Web-based Interface

By default, the IP address used to access the web-based WLAN interface is 10.10.10.2.

To change the IP address of the bridge interface used to access the web-based interface, perform these steps.

SUMMARY STEPS

1. **configure terminal**
2. **interface BVI 1**
3. **ip address** *IP-address subnet-mask*

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`ap# configure terminal`
	`ap(config)#`
		Enters configuration mode.
		Note To exit a configuration mode after completing configuration tasks, use the **exit** command as described in Modes, page 11-10.

Step 2	**interface BVI 1** **Example:** `ap(config)# interface BVI 1`	The interface number.

Step 3	**ip address** *IP-address subnet-mask*
	Example:
	`ap(config-if)# ip address 10.10.10.2`
	`255.255.255.248`
		Configures the new IP address and subnet mask.
		Note Use IPv4 addresses only.
		Tip You can display the configured IP address using the **show interfaces BVI 1** command (see Displaying the BVI 1 Interface Details, page 11-51).

Enabling and Disabling WLAN

By default, the WLAN feature is enabled.

To enable or disable WLAN, follow these steps from global configuration mode (see Configuration Mode, page 11-10):

SUMMARY STEPS

1. **interface Dot11Radio 0**
2. **[no] shutdown**

   Use **shutdown** to disable WLAN and **no shutdown** to enable WLAN.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface Dot11Radio 0** **Example:** `ap(config)# interface Dot11Radio 0`	Enters interface configuration mode.
Step 2	**[no] shutdown** **Example:** `ap(config-if)# no shutdown`	**shutdown**—Disables WLAN. **no shutdown**—Enables WLAN.

Configuring the Main SSID

By default, the main SSID for the router is called Cisco860.

To change the name of the main SSID, perform these steps.

SUMMARY STEPS

1. **configure terminal**
2. **dot11 ssid** *SSID-name*

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`ap# configure terminal`
	`ap(config)#`
		Enters configuration mode.
		Note To exit a configuration mode after completing configuration tasks, use the **exit** command as described in Modes, page 11-10.

Step 2	**dot11 ssid** *SSID-name* **Example:** `ap(config)# dot11 ssid mainssid`	*SSID-name*—The main SSID. The SSID may be up to 32 characters. In the example, the new SSID is called mainssid.

Configuring Guest SSIDs

By default, the guest SSIDs for the router are called:

Cisco860_Guest1

Cisco860_Guest2

Cisco860_Guest3

To change the name of a guest SSID, perform these steps.

SUMMARY STEPS

1. **configure terminal**
2. **dot11 guest-ssid** *guest-SSID-number SSID-name*

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`ap# configure terminal`
	`ap(config)#`
		Enters configuration mode.
		Note To exit a configuration mode after completing configuration tasks, use the **exit** command as described in Modes, page 11-10.

Step 2	**dot11 guest-ssid** *guest-SSID-number SSID-name* **Example:** `ap(config)# dot11 guest-ssid 1 guest1`	*guest-SSID-number*—Specify 1, 2, or 3 to identify the guest SSID to configure. *SSID-name*—The new SSID. The SSID may be up to 32 characters. The example specifies a new SSID of **guest1** for guest SSID number 1.

Enabling and Disabling Guest SSIDs

The main SSID cannot be disabled. However, guest SSIDs can be enabled/disabled. By default, guest SSIDs are disabled.

To enable or disable a guest SSID, follow these steps from global configuration mode:

SUMMARY STEPS

1. **interface Dot11Radio 0**
2. **[no] guest-ssid** *guest-SSID-number SSID-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface Dot11Radio 0** **Example:** `ap(config)# interface Dot11Radio 0`	Enters interface configuration mode.
Step 2	**[no] guest-ssid** *guest-SSID-number SSID-name* **Example:** `ap(config-if)# guest-ssid 1 guestssid1`	Enables the guest SSID specified by *guest-SSID-number* and *SSID-name*. *guest-SSID-number*—Specify 1, 2, or 3 to identify the guest SSID to configure. *SSID-name*—The name of the guest SSID. Entering the wrong SSID displays an error message. The **no** form of the command disables the specified guest SSID.

Hiding an Access Point

Hiding the SSID (access point) provides a small measure of security in helping to prevent unauthorized users from accessing the network. When this feature is enabled, the SSID is not broadcast, making wireless snooping more difficult.

To hide or unhide an SSID, follow these steps from global configuration mode (see Configuration Mode, page 11-10):

SUMMARY STEPS

1. **dot11 {ssid | guest-ssid}** [*guest-SSID-number*] *SSID-name*

   guest-SSID-number is required only for the **guest-ssid** option.
2. **[no] hide-ap**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**dot11 {ssid | guest-ssid}** [*guest-SSID-number*] *SSID-name* **Example:** `ap(config)# dot11 guest-ssid 1 guestssid1`	Enters SSID configuration mode for a specific SSID. The `ap(config-ssid)` prompt indicates SSID configuration mode. **ssid**—The main SSID. **guest-ssid**—A guest SSID. *guest-SSID-number*—The guest SSID number. Use this only with the **guest-ssid** option. *SSID-name*—The SSID name.
Step 2	**[no] hide-ap** **Example:** `ap(config-ssid)# hide-ap`	Hides the SSID specified in the previous step. The **no** form of the command unhides the specified SSID.

Enabling and Disabling Client Isolation

Client isolation prevents a wireless client connected to a specific SSID from communicating with other wireless clients connected to the same SSID.

To enable or disable client isolation for a specific SSID, follow these steps from global configuration mode (see Configuration Mode, page 11-10):

SUMMARY STEPS

1. **dot11 {ssid | guest-ssid}** [*guest-SSID-number*] *SSID-name*
2. **[no] isolate-clients**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**dot11** {**ssid** | **guest-ssid**} [*guest-SSID-number*] *SSID-name* **Example:** `ap(config)# dot11 guest-ssid 1 guestssid1`	Enters SSID configuration mode for a specific SSID. The `ap(config-ssid)` prompt indicates SSID configuration mode. **ssid**—The main SSID. **guest-ssid**—A guest SSID. *guest-SSID-number*—The guest SSID number. Use this only with the **guest-ssid** option. *SSID-name*—The SSID name.
Step 2	[**no**] **isolate-clients** **Example:** `ap(config-ssid)# isolate-clients`	Enables client isolation for the SSID specified in the previous step. The **no** form of the command disables client isolation for the specified SSID.

Enabling and Disabling WMM Advertise

The WiFi Multimedia (WMM) Advertise feature prioritizes media traffic to improve media transmission.

WMM Advertise is enabled by default. To enable or disable WMM Advertise for a specific SSID, follow these steps from global configuration mode (see Configuration Mode, page 11-10):

SUMMARY STEPS

1. **dot11** {**ssid** | **guest-ssid**} [*guest-SSID-number*] *SSID-name*
2. [**no**] **disable-wmm**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**dot11 {ssid | guest-ssid}** [*guest-SSID-number*] *SSID-name* **Example:** `ap(config)#` **`dot11 guest-ssid 1 guestssid1`**	Enters SSID configuration mode for a specific SSID. The `ap(config-ssid)` prompt indicates SSID configuration mode. **ssid**—The main SSID. **guest-ssid**—A guest SSID. *guest-SSID-number*—The guest SSID number. Use this only with the **guest-ssid** option. *SSID-name*—The SSID name.
Step 2	**[no] disable-wmm** **Example:** `ap(config-ssid)#` **`disable-wmm`**	Disables the WMM Advertise feature for the SSID specified in the previous step. The **no** form of the command enables the WMM Advertise feature for the specified SSID. **Note** WMM Advertise is enabled by default.

Enabling and Disabling Wireless Multicast Forwarding (WMF)

The Wireless Multicast Forwarding(WMF) feature improves multicast traffic performance.

To enable or disable Wireless Multicast Forwarding(WMF) for a specific SSID, follow these steps from global configuration mode (see Configuration Mode, page 11-10):

SUMMARY STEPS

1. **dot11 {ssid | guest-ssid}** [*guest-SSID-number*] *SSID-name*
2. **[no] wmf**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**dot11** {**ssid** | **guest-ssid**} [*guest-SSID-number*] *SSID-name* **Example:** `ap(config)# dot11 guest-ssid 1 guestssid1`	Enters SSID configuration mode for a specific SSID. The `ap(config-ssid)` prompt indicates SSID configuration mode. **ssid**—The main SSID. **guest-ssid**—A guest SSID. *guest-SSID-number*—The guest SSID number. Use this only with the **guest-ssid** option. *SSID-name*—The SSID name.
Step 2	[**no**] **wmf** **Example:** `ap(config-ssid)# wmf`	Enables the WMF feature for the SSID specified in the previous step. The **no** form of the command disables the WMF feature for the specified SSID.

Configuring the Global Maximum Number of Clients

Use the **global-max-clients** command to configure the maximum number of clients that can connect to an AP. The **max-associations** command specifies the maximum number of clients for a specific SSID (see Configuring the Maximum Number of Clients for an SSID, page 11-20); that value cannot exceed the global maximum.

To set the global maximum number of clients, follow these steps from global configuration mode (see Configuration Mode, page 11-10):

SUMMARY STEPS

1. **configure terminal**
2. **global-max-clients** *number-of-clients*

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`ap# configure terminal`
	`ap(config)#`
		Enters configuration mode.
		Note To exit a configuration mode after completing configuration tasks, use the **exit** command as described in Modes, page 11-10.

Step 2	**global-max-clients** *number-of-clients* **Example:** `ap(config)# global-max-clients 32`	Configures the maximum number of clients that can connect to an AP. *number-of-clients* range: 1 to 128 clients

Configuring the Maximum Number of Clients for an SSID

Use the **max-associations** command to configure the maximum number of clients that can connect to a specific SSID. The standard range is 1 to 128, but is limited by the global maximum configured by the **global-max-clients** command (see Configuring the Global Maximum Number of Clients, page 11-19).

To configure the maximum number of clients, follow these steps from global configuration mode (see Configuration Mode, page 11-10):

SUMMARY STEPS

1. **dot11 {ssid | guest-ssid}** [*guest-SSID-number*] *SSID-name*
2. **max-associations** *number-of-clients*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**dot11 {ssid | guest-ssid}** [*guest-SSID-number*] *SSID-name* **Example:** `ap(config)# dot11 guest-ssid 1 guestssid1`	Enters SSID configuration mode for a specific SSID. The `ap(config-ssid)` prompt indicates SSID configuration mode. **ssid**—The main SSID. **guest-ssid**—A guest SSID. *guest-SSID-number*—The guest SSID number. Use this only with the **guest-ssid** option. *SSID-name*—The SSID name.
Step 2	**max-associations** *number-of-clients* **Example:** `ap(config-ssid)# max-associations 24`	Configures the maximum number of clients for the SSID specified in the previous step. *number-of-clients*—Range 1 to 128 Default value: 16 Recommended maximum: 16 Theoretical maximum: 128 Entering a value higher than the global maximum configured by the **global-max-clients** command results in an error. For example, if the global maximum is 16, configuring a larger number results in the following error: `Entered number does not apply to the valid range : 1 - 16(global max client)`

Configuring Authentication Options

Use the **authentication** command to configure authentication options for a specific SSID. By default, network authentication is Open.

To configure the authentication options, follow these steps from global configuration mode (see Configuration Mode, page 11-10):

SUMMARY STEPS

1. **dot11 {ssid | guest-ssid}** [*guest-SSID-number*] *SSID-name*
2. **authentication** *authentication-options*
   For *authentication-options* argument values, see Table 11-2.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**dot11 {ssid | guest-ssid}** [*guest-SSID-number*] *SSID-name* **Example:** `ap(config)# dot11 guest-ssid 1 guestssid1`	Enters SSID configuration mode for a specific SSID. The `ap(config-ssid)` prompt indicates SSID configuration mode. **ssid**—The main SSID. **guest-ssid**—A guest SSID. *guest-SSID-number*—The guest SSID number. Use this only with the **guest-ssid** option. *SSID-name*—The SSID name.
Step 2	**authentication** *authentication-options* **Example:** `ap(config-ssid)# authentication open`	Configures authentication options for the SSID specified in the previous step. Table 11-2 describes options for the **authentication** command. The default authentication option is **open**.

Table 11-2 describes options for the **authentication** command:

Table 11-2 Authentication Command Options

Option	Syntax	Description
Open authentication	**open**	Configures open authentication.
Shared authentication	**shared** **Example:** `ap(config-ssid)# authentication shared`	Configures shared authentication.

Option	Syntax	Description
802.1x Options		
Authentication server port	**802.1x auth-port** *port-number* **Example:** `ap(config-ssid)# authentication 802.1x auth-port 2000`	Defines the UDP port for the RADIUS authentication server. Range: 0 to 65535 Default: 1812
RADIUS key	**802.1x key** *encryption-key* **Example:** `ap(config-ssid)# authentication 802.1x key ABC123ABC1`	Defines the per-server encryption key. Enter the server key in an unencrypted (cleartext) form.
RADIUS server address	**802.1x server** *server-IP-address* **Example:** `ap(config-ssid)# authentication 802.1x server 10.1.1.1`	Specifies a RADIUS server.
WPA Authentication		
Authentication server port	**WPA auth-port** *port-number* **Example:** `ap(config-ssid)# authentication WPA auth-port 2000`	Defines the UDP port for the RADIUS authentication server. Range: 0 to 65535 Default: 1812
RADIUS key	**WPA key** *encryption-key* **Example:** `ap(config-ssid)# authentication WPA key ABC123ABC1`	Defines the per-server encryption key. Enter the server key in an unencrypted (cleartext) form.
WPA Group Rekey Interval	**WPA rekey-interval** *seconds* **Example:** `ap(config-ssid)# authentication WPA rekey-interval 604800`	Defines the authentication rekey interval in seconds. Range: 0 to 2147483647 (seconds) The example configures the rekey interval to one week (604800 seconds).
RADIUS server address	**WPA server** *server-IP-address* **Example:** `ap(config-ssid)# authentication WPA server 10.1.1.1`	Specifies a RADIUS server.

Option	Syntax	Description
WPA-PSK Authentication		
WPA/WAPI passphrase	**WPA-PSK passphrase** *password* `ap(config-ssid)#` **`authentication WPA-PSK passphrase MyPaSsWoRd`**	The passphrase for WPA-PSK. Enter a cleartext/unencrypted WPA passphrase. Range: 8 to 63 ASCII characters or 64 hexadecimal digits
WPA Group Rekey Interval	**WPA-PSK rekey-interval** *seconds* **Example:** `ap(config-ssid)#` **`authentication WPA-PSK rekey-interval 604800`**	Defines the authentication rekey interval in seconds. Range: 0 to 2147483647 (seconds) The example configures the rekey interval to one week (604800 seconds).
WPA2 Authentication		
Authentication server port	**WPA2 auth-port** *port-number* **Example:** `ap(config-ssid)#` **`authentication WPA2 auth-port 2000`**	Defines the UDP port for the RADIUS authentication server. Range: 0 to 65535 Default: 1812
RADIUS key	**WPA2 key** *encryption-key* **Example:** `ap(config-ssid)#` **`authentication WPA2 key ABC123ABC1`**	Defines the per-server encryption key. Enter the server key in an unencrypted (cleartext) form.
WPA2 preauthentication	**WPA2 preauth** **Example:** `ap(config-ssid)#` **`authentication WPA2 preauth`** **Example:** `ap(config-ssid)#` **`no authentication WPA2 preauth`**	Enables WPA2 preauthentication. The **no** form of the command disables preauthentication.
Network reauthorization interval	**WPA2 reauth-interval** *seconds* **Example:** `ap(config-ssid)#` **`authentication WPA2 reauth-interval 604800`**	Defines the WPA2 reauthorization interval in seconds. Range: 0 to 2147483647 (seconds) The example configures the reauthorization interval to one week (604800 seconds).
WPA Group Rekey Interval	**WPA2 rekey-interval** *seconds* **Example:** `ap(config-ssid)#` **`authentication WPA2 rekey-interval 604800`**	Defines the authentication rekey interval in seconds. Range: 0 to 2147483647 (seconds) The example configures the rekey interval to one week (604800 seconds).

Option	Syntax	Description
RADIUS server address	**WPA2 server** *server-IP-address* **Example:** `ap(config-ssid)#` **`authentication WPA2 server 10.1.1.1`**	Specifies a RADIUS server.
WPA2-PSK Authentication		
WPA/WAPI passphrase	**WPA2-PSK passphrase** *password* `ap(config-ssid)#` **`authentication WPA2-PSK passphrase MyPaSsWoRd`**	The passphrase for WPA2-PSK. Enter a cleartext/unencrypted WPA passphrase. Range: 8 to 63 ASCII characters or 64 hexadecimal digits
WPA-PSK Group Rekey Interval	**WPA2-PSK rekey-interval** *seconds* **Example:** `ap(config-ssid)#` **`authentication WPA2-PSK rekey-interval 604800`**	Defines the authentication rekey interval in seconds. Range: 0 to 2147483647 (seconds) The example configures the rekey interval to one week (604800 seconds).
Mixed WPA2/WPA Authentication		
Authentication server port	**Mixed-WPA2-WPA auth-port** *port-number* **Example:** `ap(config-ssid)#` **`authentication Mixed-WPA2-WPA auth-port 2000`**	Defines the UDP port for the RADIUS authentication server. Range: 0 to 65535 Default: 1812
RADIUS key	**Mixed-WPA2-WPA key** *encryption-key* **Example:** `ap(config-ssid)#` **`authentication Mixed-WPA2-WPA key ABC123ABC1`**	Defines the per-server encryption key. Enter the server key in an unencrypted (cleartext) form.
WPA2 preauthentication	**Mixed-WPA2-WPA preauth** **Example:** `ap(config-ssid)#` **`authentication Mixed-WPA2-WPA preauth`** **Example:** `ap(config-ssid)#` **`no authentication Mixed-WPA2-WPA preauth`**	Enables WPA2 preauthentication. The **no** form of the command disables preauthentication.
Network reauthorization interval	**Mixed-WPA2-WPA reauth-interval** **Example:** `ap(config-ssid)#` **`authentication Mixed-WPA2-WPA reauth-interval 604800`**	Defines the WPA2 reauthorization interval in seconds. Range: 0 to 2147483647 (seconds) The example configures the reauthorization interval to one week (604800 seconds).

Option	Syntax	Description
WPA Group Rekey Interval	**Mixed-WPA2-WPA rekey-interval** *seconds* **Example:** `ap(config-ssid)# authentication Mixed-WPA2-WPA rekey-interval 604800`	Defines the authentication rekey interval in seconds. Range: 0 to 2147483647 (seconds) The example configures the rekey interval to one week (604800 seconds).
RADIUS server address	**Mixed-WPA2-WPA server** *server-IP-address* **Example:** `ap(config-ssid)# authentication Mixed-WPA2-WPA server 10.1.1.1`	Specifies a RADIUS server.
Mixed WPA2/WPA-PSK Authentication		
Passphrase	**Mixed-WPA2-WPA-PSK passphrase** *password* **Example:** `ap(config-ssid)# authentication Mixed-WPA2-WPA-PSK passphrase MyPaSsWoRd`	The preshared passphrase for WiFi protected access. Enter a clear WPA passphrase. Range: 8 to 63 ASCII characters or 64 hexadecimal digits
WPA Group Rekey Interval	**WPA2-PSK rekey-interval** *seconds* **Example:** `ap(config-ssid)# authentication Mixed-WPA2-WPA-PSK rekey-interval 604800`	Defines the authentication rekey interval in seconds. Range: 0 to 2147483647 (seconds) The example configures the rekey interval to one week (604800 seconds).

Configuring Encryption Options

Use the **encryption mode** command to configure encryption options for a specific SSID.

To configure the encryption options, follow these steps from global configuration mode (see Configuration Mode, page 11-10):

SUMMARY STEPS

1. **dot11 {ssid | guest-ssid}** [*guest-SSID-number*] *SSID-name*
2. **encryption mode** *encryption-options*
   For *encryption-options*, see Table 11-3.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**dot11** {**ssid** | **guest-ssid**} [*guest-SSID-number*] *SSID-name* **Example:** `ap(config)# dot11 guest-ssid 1 guestssid1`	Enters SSID configuration mode for a specific SSID. The `ap(config-ssid)` prompt indicates SSID configuration mode. **ssid**—The main SSID. **guest-ssid**—A guest SSID. *guest-SSID-number*—The guest SSID number. Use this only with the **guest-ssid** option. *SSID-name*—The SSID name.
Step 2	**encryption mode** *encryption-options* **Example:** `ap(config-ssid)# encryption mode wep`	Configures encryption options for the SSID specified in the previous step. Table 11-3 describes options for the **encryption mode** command.

Table 11-3 describes options for the **encryption mode** command:

Table 11-3 Encryption Command Options

Option	Syntax	Description
WEP encryption options		

Enable/Disable WEP encryption	**[no] encryption mode wep**
	Example:
	`ap(config-ssid)# encryption mode wep`
	Example:
	`ap(config-ssid)# no encryption mode wep`
		Enables WEP encryption. The **no** form of the command disables WEP encryption.
		Note The WEP encryption default setting depends on the authentication option selected.
		Open authentication—Default is disabled.
		Shared—Default is enabled; cannot disable.
		802.1x—Default is enabled; cannot disable.
		WPA, WPA-PSK, WPA2, WPA2-PSK, Mixed WPA2/WPA, Mixed WPA2/WPA-PSK—Default is disabled; cannot enable.

Option	Syntax	Description
Encryption strength	**wep encryption-strength [64bit | 128bit]** **Example:** `ap(config-ssid)#` **`encryption mode wep encryption-strength 64bit`**	Configures the WEP encryption strength. **64bit**—Specifies a 64-bit key. **128bit**—Specifies a 128-bit key.
Current network key	**wep current-key** *key-number* **Example:** `ap(config-ssid)#` **`encryption mode wep current-key 1`**	It is possible to configure four different network keys. This command determines which key to use currently. *key-number* range: 1 to 4
Network key	**wep key** *key-number key* **Example:** `ap(config-ssid)#` **`encryption mode wep key 1 54321`**	Configures a network key. *key-number* range: 1 to 4 *key*: • For a 64-bit key: 5 ASCII characters or 10 hexadecimal digits • For a 128-bit key: 13 ASCII characters or 26 hexadecimal digits
WPA/WAPI Encryption Options		
AES	**aes** **Example:** `ap(config-ssid)#` **`encryption mode aes`**	Configures the encryption mode to AES. **Note** AES is supported only under WPA, WPA-PSK, WPA2, WPA2-PSK, Mixed WPA2/WPA, or Mixed WPA2/WPA-PSK.
TKIP+AES	**tkip+aes** **Example:** `ap(config-ssid)#` **`encryption mode tkip+aes`**	Configures the encryption mode to TKIP+AES. **Note** TKIP+AES is supported only under WPA, WPA-PSK, WPA2, WPA2-PSK, Mixed WPA2/WPA, or Mixed WPA2/WPA-PSK.

Configuring the MAC Address Filter Access List

Use the **access-list** command to create an "access list" for MAC address filtering for a specific SSID. The access list contains device MAC addresses, to allow only those devices to connect to the SSID or to deny the devices access to the SSID. Use the **mac-filter-mode** command to select the mode for handling the access list (disable, allow, or deny)—see Configuring the MAC Address Filter Mode, page 11-28.

To add a MAC address to the list or to remove a MAC address from the list, follow these steps from global configuration mode (see Configuration Mode, page 11-10):

SUMMARY STEPS

1. **dot11 {ssid | guest-ssid}** [*guest-SSID-number*] *SSID-name*
2. **[no] access-list** *MAC-address*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**dot11 {ssid | guest-ssid}** [*guest-SSID-number*] *SSID-name* **Example:** `ap(config)# dot11 guest-ssid 1 guestssid1`	Enters SSID configuration mode for a specific SSID. The `ap(config-ssid)` prompt indicates SSID configuration mode. **ssid**—The main SSID. **guest-ssid**—A guest SSID. *guest-SSID-number*—The guest SSID number. Use this only with the **guest-ssid** option. *SSID-name*—The SSID name.

Step 2	**[no] access-list** *MAC-address*
	Example:
	`ap(config-ssid)# access-list AB:12:CD:34:EF:56`
	Example:
	`ap(config-ssid)# no access-list AB:12:CD:34:EF:56`
		Adds the MAC address to the access list for the SSID specified in the previous step.
		MAC-address—Hexadecimal characters in the following format: HH:HH:HH:HH:HH:HH
		The **no** form of the command removes a MAC address from the access list.

Configuring the MAC Address Filter Mode

Use the **mac-filter-mode** command to select the mode for handling the access list:

- Disable—Disables the access list.
- Allow—Allows devices specified in the access list to connect to the SSID.
- Deny—Denies devices specified in the access list from connecting to the SSID.

For information about creating the access list, see Configuring the MAC Address Filter Access List, page 11-27.

To select the MAC address access list mode, follow these steps from global configuration mode (see Configuration Mode, page 11-10):

SUMMARY STEPS

1. **dot11 {ssid | guest-ssid}** [*guest-SSID-number*] *SSID-name*
2. **[no] mac-filter-mode [allow | deny]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**dot11** {**ssid** | **guest-ssid**} [*guest-SSID-number*] *SSID-name* **Example:** `ap(config)# dot11 guest-ssid 1 guestssid1`	Enters SSID configuration mode for a specific SSID. The `ap(config-ssid)` prompt indicates SSID configuration mode. **ssid**—The main SSID. **guest-ssid**—A guest SSID. *guest-SSID-number*—The guest SSID number. Use this only with the **guest-ssid** option. *SSID-name*—The SSID name.

Step 2	[**no**] **mac-filter-mode** [**allow** | **deny**]
	Example:
	`ap(config-ssid)# mac-filter-mode allow`
	Example:
	`ap(config-ssid)# mac-filter-mode deny`
	Example:
	`ap(config-ssid)# no mac-filter-mode`
		Configures the mode for the MAC address filter feature.
		To allow MAC addresses on the access list to connect:
		mac-filter-mode allow
		To deny MAC addresses on the access list from connecting:
		mac-filter-mode deny
		To disable the feature:
		no mac-filter-mode

Advanced Options: Configuring Radio Channel

Use the **channel** command to configure radio channel options:

- Manually specify a channel.
- Automatically scan for the best (least congested) channel to use.

To configure channel options, follow these steps from global configuration mode (see Configuration Mode, page 11-10):

SUMMARY STEPS

1. **interface Dot11Radio 0**
2. **channel** {*channel-number* | **least-congested**} [**timer** *minutes-before-next-scan*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface Dot11Radio 0** **Example:** `ap(config)# interface Dot11Radio 0`	Enters radio interface mode, indicated by the `ap(config-if)` prompt.

Step 2	**channel** {*channel-number* | **least-congested**} [**timer** *minutes-before-next-scan*]
	Example:
	`ap(config-if)# channel 1`
	Example:
	`ap(config-if)# channel least-congested timer 60`
		Configures a specific radio channel manually or selects automatic scanning; and configures the automatic scanning timer.
		To set a specific channel:
		channel *channel-number*
		channel-number range: 1 to11 for American models, or 1 to 13 for European models
		To configure automatic scanning for the least congested channel, use the **least-congested** option and specify the number of minutes to wait before scanning again for the best channel:
		channel least-congested timer *minutes-before-next-scan*
		minutes-before-next-scan range: 1 to 35791394

Advanced: Configuring 802.11n Options

Use the **dot11n** command to configure 802.11n options.

To configure 802.11n options, follow these steps from global configuration mode (see Configuration Mode, page 11-10):

SUMMARY STEPS

1. **interface Dot11Radio 0**
2. **[no] dot11n [rate | protection | n-client-only | rifs | rx-pwr-save | rx-pwr-save quiet-time | pps]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface Dot11Radio 0** **Example:** `ap(config)#` **`interface Dot11Radio 0`**	Enters radio interface mode, indicated by the `ap(config-if)` prompt.
Step 2	**[no] dot11n**	**Enable/Disable 802.11n** Configures 802.11n radio options. To enable 802.11n: **dot11n** To disable 802.11n: **no dot11n**
	dot11n rate	**Rate** To configure the 802.11n rate: **dot11n {***rate* **| 54g | auto}** *rate* range: 0 to 15. Table 11-4 describes the 802.11n rates for each *rate* value. **54g**—Uses the 54g rate. **auto**—Selects a rate automatically.
	[no] dot11n protection	**Protection** To enable 802.11n protection: **dot11n protection** To disable 802.11n protection: **no dot11n protection**

	Command or Action	Purpose
	[no] dot11n n-client-only	**N-client-only Mode** To enable 802.11n client-only mode, which limits the WLAN to clients using 802.11n: **dot11n n-client-only** To disable 802.11n client-only mode: **no dot11n n-client-only** **Note** When the 802.11n client-only option is enabled, clients are unable to connect to SSIDs with a WEP security setting. To enable the client to connect to the SSID, change the SSID security setting so that WEP is not configured. Alternatively, the client can connect to an SSID with non-WEP security settings.

<table>
<tr><th></th><th>Command or Action</th><th>Purpose</th></tr>
<tr><td></td><td><b>[no] dot11n rifs</b></td><td><b>RIFS Advertisement</b>
To enable Reduced Inter-Frame Space (RIFS) advertisement:
<b>dot11n rifs</b></td></tr>
<tr><td></td><td><b>[no] dot11n [rx-pwr-save | rx-pwr-save quiet-time | pps]</b></td><td><b>RX Chain Power Save (power save mode)</b>
To enable RX Chain Power Save:
<b>dot11n rx-pwr-save</b>
To disable RX Chain Power Save:
<b>no dot11n rx-pwr-save</b>
To set the RX Chain Power Save quiet time (time interval to wait before going into power save mode):
<b>dot11n rx-pwr-save quiet-time <i>seconds</i></b>
<i>seconds</i> range: 0 to 2147483647
Power Save packets per second (pps) threshold:
When the pps is below this threshold, the router enters power save mode after the number of seconds configured for the “RX Chain Power Save Quiet Time” value.
To set the RX Chain Power Save packets per second threshold:
<b>dot11n rx-pwr-save pps <i>pps-value</i></b>
<i>pps-value</i> range: 0 to 2147483647 packets per second</td></tr>
</table>

Table 11-4 describes the rate options for 802.11n, as specified by rate in the **dot11n** *rate* command:

Table 11-4 Rate Options for 802.11n

Value	Rate
0	MCS index 0, 6.5 Mbps
1	MCS index 1, 13 Mbps
2	MCS index 2, 19.5 Mbps
3	MCS index 3, 26 Mbps
4	MCS index 4, 39 Mbps
5	MCS index 5, 52 Mbps
6	MCS index 6, 58.5 Mbps

Value	Rate
7	MCS index 7, 65 Mbps
8	MCS index 8, 13 Mbps
9	MCS index 9, 26 Mbps
10	MCS index 10, 39 Mbps
11	MCS index 11, 52 Mbps
12	MCS index 12, 78 Mbps
13	MCS index 13, 104 Mbps
14	MCS index 14, 117 Mbps
15	MCS index 15, 130 Mbps

Advanced: Configuring the 54g Mode

Use the **54g-mode** command to configure the 54g mode.

To set the 54g mode, follow these steps from global configuration mode (see Configuration Mode, page 11-10):

SUMMARY STEPS

1. **interface Dot11Radio 0**
2. **54g-mode [auto | dot11b-only | lrs | performance]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface Dot11Radio 0** **Example:** `ap(config)# interface Dot11Radio 0`	Enters radio interface mode, indicated by the `ap(config-if)` prompt.
Step 2	**54g-mode [auto | dot11b-only | lrs | performance]** **Example:** `ap(config-if)# 54g-mode auto`	Configures the 54g mode. **auto**—54g auto mode. Accepts 802.11b, 802.11g, and 54g clients. This option provides the widest compatibility. **dot11b-only**—Accepts only 802.11b clients. **lrs**—54g Limited Rate Support (LRS). Intended for legacy 802.11b client support. **performance**—54g Performance mode. Accepts only 54g clients, provides the fastest performance with 54g certified equipment.

Advanced: Configuring the 54g Preamble Type

Use the **54g-mode preamble** command to configure the 54g preamble type. The preamble type can be set only when 802.11n is disabled (**no dot11n**) and 54g-mode is either **auto** or **dot11b-only**. For information about setting 54g mode, see Advanced: Configuring the 54g Mode, page 11-34.

To set the 54g preamble type, follow these steps from global configuration mode (see Configuration Mode, page 11-10):

SUMMARY STEPS

1. **interface Dot11Radio 0**
2. **54g-mode {auto | dot11b-only} preamble {short | long}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface Dot11Radio 0** **Example:** `ap(config)# interface Dot11Radio 0`	Enters radio interface mode, indicated by the `ap(config-if)` prompt.

Step 2	**54g-mode {auto	dot11b-only} preamble {short	long}**
			Example:
			`ap(config-if)# 54g-mode auto preamble long`
			Example:
			`ap(config-if)# 54g-mode dot11b-only preamble short`
				Configures 54g preamble type.
				short—Short preamble. When there are no 802.11b clients, setting preamble type to **short** improves performance.
				long—Long preamble. When there are both 802.11g and 802.11b clients, set preamble type to **long**.
				Note **54g-mode** must be either **auto** or **dot11b-only**.

Advanced: Configuring the 54g Rate

Use the **54g-rate** command to configure the 54g transmission rate. The 54g rate can be set only when the 802.11n rate is configured to use 54g rate (**dot11n rate 54g**) or when 802.11n is disabled (**no dot11n**).

To set the 54g rate, follow these steps from global configuration mode (see Configuration Mode, page 11-10):

SUMMARY STEPS

1. **interface Dot11Radio 0**
2. **54g-rate** {*Mbps-rate* | **auto**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface Dot11Radio 0** **Example:** `ap(config)#` **`interface Dot11Radio 0`**	Enters radio interface mode, indicated by the `ap(config-if)` prompt.

Step 2	**54g-rate** {*Mbps-rate* |**auto**}
	Example:
	`ap(config-if)#` **`54g-rate 54`**
	Example:
	`ap(config-if)#` **`54g-rate auto`**
		Configures the rate for 54g mode.
		Mbps-rate specifies a rate in Mbps. The following values are possible:
		1
		2
		5.5
		6
		9
		11
		12
		18
		24
		36
		48
		54
		auto—Sets the 54g rate automatically.

Advanced: Configuring 54g Protection

Use the **54g-protection** command to enable 54g protection. This can be set only when 802.11n is disabled (**no dot11n**).

To set 54g protection, follow these steps from global configuration mode (see Configuration Mode, page 11-10):

SUMMARY STEPS

1. **interface Dot11Radio 0**
2. **54g-protection**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface Dot11Radio 0** **Example:** `ap(config)# interface Dot11Radio 0`	Enters radio interface mode, indicated by the `ap(config-if)` prompt.
Step 2	**54g-protection** **Example:** `ap(config-if)# 54g-protection`	Enables 54g protection. **54g-protection**—Enables the RTS/CTS protection mechanism. **no 54g-protection**—Disables 54g protection.

Advanced: Configuring the Multicast Rate

Use the **multicast-rate** command to configure the transmit/receive rate for multicast packets.

If 802.11n is disabled and 54g-mode is set to 802.11b, then in the CLI, attempting to set the multicast rate to anything other than auto, 1, 2, 5.5, or 11 Mbps will cause the following error message to be displayed:

```
Only auto, 1, 2, 5.5 or 11 Mbps is available when "no dot11n" has been issued and 54g
mode is 802.11b only.
```

To set the multicast transmission rate, follow these steps from global configuration mode (see Configuration Mode, page 11-10):

SUMMARY STEPS

1. **interface Dot11Radio 0**
2. **multicast-rate** {*Mbps-rate* |**auto**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface Dot11Radio 0** **Example:** `ap(config)# interface Dot11Radio 0`	Enters radio interface mode, indicated by the `ap(config-if)` prompt.

Step 2	**multicast-rate** {*Mbps-rate* | **auto**}
	Example:
	`ap(config-if)# multicast-rate 54`
	Example:
	`ap(config-if)# multicast-rate auto`
		Configures the multicast rate.
		Mbps-rate specifies a rate in Mbps. The following values are possible:
		1
		2
		5.5
		6
		9
		11
		12
		18
		24
		36
		48
		54
		auto—Sets the multicast rate automatically.
		Note When 802.11n is disabled (**no dot11n**) and 54g-mode is configured to 802.11b only (**54g-mode dot11b-only**), the only accepted rates are auto, 1, 2, 5.5, or 11 Mbps. Attempting to configure any other rate displays the following warning message:
		`Only auto, 1, 2, 5.5 or 11 Mbps is available when "no dot11n" has been issued and 54g mode is 802.11b only.`

Advanced: Configuring the Basic Rate

Use the **basic-rate** command to configure the basic transmission rate, which is the data rate that wireless clients should support.

To set the basic transmission rate, follow these steps from global configuration mode (see Configuration Mode, page 11-10):

SUMMARY STEPS

1. **interface Dot11Radio 0**
2. **basic-rate {1 | 2 | all | default}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface Dot11Radio 0** **Example:** `ap(config)# interface Dot11Radio 0`	Enters radio interface mode, indicated by the `ap(config-if)` prompt.

Step 2	**basic-rate {1 | 2 | all | default}**
	Example:
	`ap(config-if)# basic-rate 2`
	Example:
	`ap(config-if)# basic-rate all`
		Configures the basic rate.
		1—1 and 2 Mbps
		2—1, 2, 5.5, 6, 11, 12, and 24 Mbps
		all—All rates
		default—1, 2, 5.5, and 11 Mbps

Advanced: Configuring the Fragmentation Threshold

Use the **fragment-threshold** command to configure the fragmentation threshold, which is the maximum packet size (bytes) before data is fragmented.

To set the fragmentation threshold, follow these steps from global configuration mode (see Configuration Mode, page 11-10):

SUMMARY STEPS

1. **interface Dot11Radio 0**
2. **fragment-threshold** *threshold-in-bytes*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface Dot11Radio 0** **Example:** `ap(config)# interface Dot11Radio 0`	Enters radio interface mode, indicated by the `ap(config-if)` prompt.
Step 2	**fragment-threshold** *threshold-in-bytes* **Example:** `ap(config-if)# fragment-threshold 2346`	Configures the fragmentation threshold in bytes. *threshold-in-bytes* range: 256 to 2346 bytes Default: 2346

Advanced: Configuring the RTS Threshold

Use the **rts-threshold** command to configure the RTS (request-to-send) threshold. If an access point transmits a packet larger than the threshold, it will trigger CTS (clear-to-send) protection mode.

To set the RTS threshold, follow these steps from global configuration mode (see Configuration Mode, page 11-10):

SUMMARY STEPS

1. **interface Dot11Radio 0**
2. **rts-threshold** *threshold-in-bytes*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface Dot11Radio 0** **Example:** `ap(config)# interface Dot11Radio 0`	Enters radio interface mode, indicated by the `ap(config-if)` prompt.
Step 2	**rts-threshold** *threshold-in-bytes* **Example:** `ap(config-if)# rts-threshold 2347`	Configures the RTS threshold in bytes. *threshold-in-bytes* range: 0 to 2347 bytes Default: 2347

Advanced: Configuring the DTIM Interval

Use the **dtim-interval** command to configure the Delivery Traffic Indication Message (DTIM) interval. DTIM interval information is included in beacon frames to inform clients of when next to expect buffered data from the AP. The interval is specified as number of beacons. For example, if DTIM interval is set to 2, the client will wake up/check for buffered data on the AP at every second beacon.

To set the DTIM interval, follow these steps from global configuration mode (see Configuration Mode, page 11-10):

SUMMARY STEPS

1. **interface Dot11Radio 0**
2. **dtim-interval** *number-of-beacons*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface Dot11Radio 0** **Example:** `ap(config)# interface Dot11Radio 0`	Enters radio interface mode, indicated by the `ap(config-if)` prompt.
Step 2	**dtim-interval** *number-of-beacons* **Example:** `ap(config-if)# dtim-interval 255`	Configures the DTIM interval. *number-of-beacons* range: 1 to 255 beacons Default: 1

Advanced: Configuring the Beacon Interval

Use the **beacon-interval** command to configure the beacon interval, which is the length of time between beacon transmissions.

To set the beacon interval, follow these steps from global configuration mode (see Configuration Mode, page 11-10):

SUMMARY STEPS

1. **interface Dot11Radio 0**
2. **beacon-interval** *number-of-milliseconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface Dot11Radio 0** **Example:** `ap(config)# interface Dot11Radio 0`	Enters radio interface mode, indicated by the `ap(config-if)` prompt.
Step 2	**beacon-interval** *number-of-milliseconds* **Example:** `ap(config-if)# beacon-interval 65535`	Configures the beacon interval. *number-of-milliseconds* range: 1 to 65535 milliseconds (ms) Default: 100 ms

Advanced: Configuring the Radio Transmit Power

Use the **tx-pwr** command to set the radio transmit power for WLAN.

To set the transmit power, follow these steps from global configuration mode (see Configuration Mode, page 11-10):

SUMMARY STEPS

1. **interface Dot11Radio 0**
2. **tx-pwr** *power-percentage*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface Dot11Radio 0** **Example:** `ap(config)# interface Dot11Radio 0`	Enters radio interface mode, indicated by the `ap(config-if)` prompt.
Step 2	**tx-pwr** *power-percentage* **Example:** `ap(config-if)# tx-pwr 60`	Configures the transmit power, as a percentage of the maximum power. *power-percentage* specifies the power percentage. The following values are possible: 20 40 60 80 100

Advanced: Configuring WMM Options

Use the **wmm** command to configure WiFi Multimedia (WMM) options. By default, WMM is enabled.

To configure WMM options, follow these steps from global configuration mode (see Configuration Mode, page 11-10):

SUMMARY STEPS

1. **interface Dot11Radio 0**
2. **[no] wmm [auto | no-ack | apsd]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface Dot11Radio 0** **Example:** `ap(config)# interface Dot11Radio 0`	Enters radio interface mode, indicated by the `ap(config-if)` prompt.
Step 2	**[no] wmm [auto	no-ack	apsd]** **Example:** `ap(config-if)# wmm`	**Enable/Disable** To enable WMM: **wmm** To disable WMM: **no wmm**
	Example: `ap(config-if)# wmm auto`	**Auto Mode** To configure WMM auto mode: **wmm auto**

	Command or Action	Purpose
	Example: `ap(config-if)# wmm no-ack`	**WMM No-Acknowledgement** To configure no-acknowledgement for WMM: **wmm no-ack** To disable the no-acknowledgement feature for WMM: **no wmm no-ack** **Note** To use this option, WMM must be set to “enabled” or “auto”.
	Example: `ap(config-if)# wmm apsd`	**Automatic Power Save Delivery (APSD)** To enable APSD for WMM: **wmm apsd** To disable APSD for WMM: **no wmm apsd** **Note** When WMM is in “Auto” mode, WMM APSD must be set to “Enabled” to enable a client to use Power Save Mode. When WMM is in “Enabled” mode, the client can use Power Save Mode regardless of whether WMM APSD is “Enabled” or “Disabled”.

Displaying Current CLI Values and Keywords

Use the **show ap-config** command to display the current CLI values and keywords.

SUMMARY STEPS

1. **show ap-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show ap-config** **Example:** `ap# show ap-config`	Displays the current CLI values and keywords.

Example

```
ap# show ap-config
global-max-clients 16

dot11 ssid Cisco860
no isolate-clients
no wmf
max-associations 16
no hide-ap
no disable-wmm
no mac-filter-mode
authentication open
no encryption mode wep
exit

dot11 guest-ssid 1 Cisco860_Guest1
no isolate-clients
no wmf
max-associations 16
no hide-ap
no disable-wmm
no mac-filter-mode
authentication open
no encryption mode wep
exit

dot11 guest-ssid 2 Cisco860_Guest2
no isolate-clients
no wmf
max-associations 16
no hide-ap
no disable-wmm
no mac-filter-mode
authentication open
no encryption mode wep
exit

dot11 guest-ssid 3 Cisco860_Guest3
no isolate-clients
no wmf
max-associations 16
no hide-ap
no disable-wmm
no mac-filter-mode
authentication open
no encryption mode wep
exit
```

```
interface Dot11Radio 0
no shutdown
ssid Cisco860
no guest-ssid 1 Cisco860_Guest1
no guest-ssid 2 Cisco860_Guest2
no guest-ssid 3 Cisco860_Guest3
dot11n
channel least-congested timer 15
dot11n rate auto
dot11n protection
no dot11n n-client-only
dot11n rifs
no dot11n rx-pwr-save
dot11n rx-pwr-save quiet-time 10
dot11n rx-pwr-save pps 10
54g-rate auto
multicast-rate auto
basic-rate default
fragment-threshold 2346
rts-threshold 2347
dtim-interval 1
beacon-interval 100
tx-pwr 100
wmm
no wmm no-ack
wmm apsd
exit

interface BVI 1
ip address 10.10.10.2  255.255.255.248
no shutdown
exit
```

Displaying Current Channel and Power Information

Use the **show controllers Dot11Radio 0** command to display the current channel and power information.

SUMMARY STEPS

1. **show controllers Dot11Radio 0**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show controllers Dot11Radio 0** **Example:** `ap# show controllers Dot11Radio 0`	Displays the current channel and power information.

Example

```
ap# show controllers Dot11Radio 0
interface Dot11Radio0
Beacon Interval(ms)                 : 100

DTIM Interval(beacon)               :   1

Power Control:         On, HW
Current Channel:       11
BSS Channel:           11
BSS Local Max:         30.0 dBm
BSS Local Constraint:  0.0 dB
Channel Width:         20MHz
User Target:           31.75 dBm
SROM Antgain 2G:       2.0 dB
SROM Antgain 5G:       2.0 dB
SAR:                   -
Current rate:          [MCS15] ht mcs 15 Tx Exp 0 BW 20 sgi

Regulatory Limits:
Rate                  Chains 20MHz
DSSS                   1     19.0
OFDM                   1     13.50
MCS0_7                 1     13.50
VHT8_9SS1              1     -
DSSS_MULTI1            2     -
OFDM_CDD1              2     10.50
MCS0_7_CDD1            2     10.50
VHT8_9SS1_CDD1         2     -
MCS0_7_STBC            2     10.50
VHT8_9SS1_STBC         2     -
MCS8_15                2     10.50
VHT8_9SS2              2     -
DSSS_MULTI2            3     -
OFDM_CDD2              3     -
MCS0_7_CDD2            3     -
VHT8_9SS1_CDD2         3     -
MCS0_7_STBC_SPEXP1     3     -
VHT8_9SS1_STBC_SPEXP1  3     -
MCS8_15_SPEXP1         3     -
VHT8_9SS2_SPEXP1       3     -
MCS16_23               3     -
VHT8_9SS3              3     -

Core Index:            0
Board Limits:
Rate                  Chains 20MHz
DSSS                   1     17.50
OFDM                   1     17.50
MCS0_7                 1     17.50
VHT8_9SS1              1     -
DSSS_MULTI1            2     17.50
OFDM_CDD1              2     17.50
MCS0_7_CDD1            2     17.50
VHT8_9SS1_CDD1         2     -
MCS0_7_STBC            2     17.50
VHT8_9SS1_STBC         2     -
MCS8_15                2     17.50
VHT8_9SS2              2     -
DSSS_MULTI2            3     -
OFDM_CDD2              3     -
MCS0_7_CDD2            3     -
VHT8_9SS1_CDD2         3     -
```

```
MCS0_7_STBC_SPEXP1     3     -
VHT8_9SS1_STBC_SPEXP1  3     -
MCS8_15_SPEXP1         3     -
VHT8_9SS2_SPEXP1       3     -
MCS16_23               3     -
VHT8_9SS3              3     -

Power Targets:
Rate                  Chains 20MHz
DSSS                   1     16.0
OFDM                   1     12.0
MCS0_7                 1     12.0
VHT8_9SS1              1      8.0
DSSS_MULTI1            2      8.0
OFDM_CDD1              2      9.0
MCS0_7_CDD1            2      9.0
VHT8_9SS1_CDD1         2      8.0
MCS0_7_STBC            2      9.0
VHT8_9SS1_STBC         2      8.0
MCS8_15                2      9.0
VHT8_9SS2              2      8.0
DSSS_MULTI2            3     -
OFDM_CDD2              3     -
MCS0_7_CDD2            3     -
VHT8_9SS1_CDD2         3     -
MCS0_7_STBC_SPEXP1     3     -
VHT8_9SS1_STBC_SPEXP1  3     -
MCS8_15_SPEXP1         3     -
VHT8_9SS2_SPEXP1       3     -
MCS16_23               3     -
VHT8_9SS3              3     -

Maximum Power Target among all rates:   16.0  16.0
Last est. power                     :   0.0  15.75
Power Target for the current rate   :   16.0  16.0
Last adjusted est. power            :   0.0  15.75

Power Percentage                    :   100

Channel Status:
No scan in progress.
current mac channel     11
target channel  11
```

Displaying Current Associated Clients

Use the **show dot11 associations** command to display the current associated clients.

SUMMARY STEPS

1. **show dot11 associations**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show dot11 associations** **Example:** `ap# show dot11 associations`	Displays the current associated clients.

Example

```
ap# show dot11 associations
Authenticated      Associated      Authorized       Interface
AA:BB:CC:11:22:33  yes             no               Dot11Radio0
```

Displaying the SSID to BSSID Mapping

Each SSID has an associated BSSID. Use the **show dot11 bssid** command to display the SSID to BSSID mapping.

SUMMARY STEPS

1. **show dot11 bssid**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show dot11 bssid** **Example:** `ap# show dot11 bssid`	Displays the SSID to BSSID mapping.

Example

```
ap# show dot11 bssid
Interface       BSSID              Guest           SSID
Dot11Radio0     A4:93:4C:01:7A:9A  No              Cisco860
Dot11Radio0     A4:93:4C:01:7A:9B  Yes             Cisco860_Guest1
Dot11Radio0     A4:93:4C:01:7A:9C  Yes             Cisco860_Guest2
Dot11Radio0     A4:93:4C:01:7A:9D  Yes             Cisco860_Guest3
```

Displaying the Tx/Rx Statistics

Use the **show dot11 statistics** command to display the current transmit/receive (tx/rx) statistics for Dot11Radio 0 interface.

SUMMARY STEPS

1. **show dot11 statistics**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show dot11 statistics** **Example:** `ap# show dot11 statistics`	Displays the current tx/rx statistics for Dot11Radio 0 interface.

Example

```
ap# show dot11 statistics
            rx bytes   rx pkts   rx errs  rx drops  tx bytes   tx pkts   tx errs  tx drops
Dot11Radio0        0         0         0         0     12824        94         0         0
```

Displaying the BVI 1 Interface Details

Use the **show interfaces BVI 1** command to display BVI 1 interface details. Details include the IP address of the router.

Tip After changing the IP address used for accessing the router, this command can be used to confirm the change. See Setting the IP Address for the Web-based Interface, page 11-12.

SUMMARY STEPS

1. **show interfaces BVI 1**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show interfaces BVI 1** **Example:** `ap# show interfaces BVI 1`	Displays the current BVI 1 interface details.

Example

```
ap# show interfaces BVI 1
BVI1
          Link encap:Ethernet  HWaddr AA:11:BB:22:CC:33
          inet addr:10.10.10.2  Bcast:10.10.10.7  Mask:255.255.255.248
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:260 multicast:86 unicast:0 broadcast:174
          RX errors:0 dropped:0 overruns:0 frame:0
          TX packets:21 multicast:0 unicast:21 broadcast:0
          TX errors:0 dropped:0 overruns:0 carrier:0 collisions:0
          txqueuelen:0
          RX bytes:46642 (45.5 KiB) TX bytes:1260 (1.2 KiB)
          RX multicast bytes:32164 (31.4 KiB) TX multicast bytes:0 (0.0 B)
```

Displaying Dot11Radio 0 Interface Information

Use the **show interfaces Dot11Radio 0** command to display Dot11Radio 0 interface information.

SUMMARY STEPS

1. **show interfaces Dot11Radio 0**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show interfaces Dot11Radio 0** **Example:** `ap# show interfaces Dot11Radio 0`	Displays the current Dot11Radio 0 interface information.

Example

```
ap# show interfaces Dot11Radio 0
Dot11Radio0
          Link encap:Ethernet  HWaddr AA:11:BB:22:CC:33
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 multicast:0 unicast:0 broadcast:0
          RX errors:0 dropped:0 overruns:0 frame:160876
          TX packets:267 multicast:86 unicast:0 broadcast:181
          TX errors:0 dropped:0 overruns:0 carrier:0 collisions:0
          txqueuelen:1000
          RX bytes:0 (0.0 B) TX bytes:52150 (50.9 KiB)
          RX multicast bytes:0 (0.0 B) TX multicast bytes:0 (0.0 B)
          Interrupt:15 Base address:0x4000
```

Displaying Brief Details for All Interfaces

Use the **show ip interface brief** command to display brief details for all interfaces.

SUMMARY STEPS

1. **show ip interface brief**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show ip interface brief** **Example:** `ap# show ip interface brief`	Displays brief details for all interfaces.

Example

In the output, the Method column indicates whether the interface was user-configured or configured by DHCP.

```
ap# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Dot11Radio0                unassigned      YES NVRAM  up                    up
BVI1                       10.10.10.2      YES NVRAM  up                    up
```

Displaying CPU Statistics

Use the **show processes cpu** command to display CPU utilization statistics.

SUMMARY STEPS

1. **show processes cpu**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show processes cpu** **Example:** `ap# show processes cpu`	Displays CPU utilization statistics.

Example

```
ap# show processes cpu
CPU:   0% usr   0% sys   0% nic  90% idle   0% io   0% irq   9% sirq
```

Showing a Summary of Memory Usage

Use the **show memory summary** command to display details of current memory usage.

SUMMARY STEPS

1. **show memory summary**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show memory summary** **Example:** `ap# show memory summary`	Displays details of current memory usage.

Example

```
ap# show memory summary
                Total(kB)       Used(kB)       Free(kB)
Processor           88052          44212          43840
```

Pinging an Address

Use the **ping** command to test connectivity with a specific address.

SUMMARY STEPS

1. **ping** {*IP-address* | *hostname*}

DETAILED STEPS

	Command or Action	Purpose

Step 1	**ping** {*IP-address* | *hostname*}
	Example:
	`ap# ping 10.0.0.0`
		Tests connectivity to the specified IP address or host name.
		Entering the **ping** command with an address specified indicates the round trip time in milliseconds for several transmissions of a small datagram.
		Entering the **ping** command without specifying an address starts the interactive mode of the command, enabling you to enter the target address, the transmission repeat count, and the datagram size.

Example—Standard

```
ap# ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1): 100 data bytes
108 bytes from 10.10.10.1: seq=0 ttl=64 time=0.566 ms
108 bytes from 10.10.10.1: seq=1 ttl=64 time=0.195 ms
108 bytes from 10.10.10.1: seq=2 ttl=64 time=0.195 ms
108 bytes from 10.10.10.1: seq=3 ttl=64 time=0.195 ms
108 bytes from 10.10.10.1: seq=4 ttl=64 time=0.194 ms

--- 10.10.10.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.194/0.269/0.566 ms
```

Example—Interactive Mode

```
ap# ping
Target IP address: 10.10.10.1
Repeat count [5]: 6
Datagram size [100]: 150
PING 10.10.10.1 (10.10.10.1): 150 data bytes
158 bytes from 10.10.10.1: seq=0 ttl=64 time=0.358 ms
158 bytes from 10.10.10.1: seq=1 ttl=64 time=0.200 ms
158 bytes from 10.10.10.1: seq=2 ttl=64 time=0.198 ms
158 bytes from 10.10.10.1: seq=3 ttl=64 time=0.201 ms
158 bytes from 10.10.10.1: seq=4 ttl=64 time=0.197 ms
158 bytes from 10.10.10.1: seq=5 ttl=64 time=0.197 ms

--- 10.10.10.1 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0.197/0.225/0.358 ms
```

Changing the Administrator Password

Use the **password** command to change the administrator password.

Note The default login credentials are:
User name: **admin**
Password: **admin**

When logging in for the first time, the router prompts you to change the default password.

SUMMARY STEPS

1. **password** *old-password new-password confirm-password*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**password** *old-password new-password confirm-password* **Example:** `ap# password admin AbCdE123# AbCdE123#`	Changes the administrator password. Note that the command requires entering the new password twice to confirm the exact text of the new password.

Configuring the Number of Lines on Screen

Use the **terminal length** command to configure the number of lines displayed on the screen.

SUMMARY STEPS

1. **terminal length** *number-of-lines*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**terminal length** *number-of-lines* **Example:** `ap# terminal length 40`	Sets the number of lines displayed on the screen. *number-of-lines* range: 0 to 512 A value of 0 specifies that the display does not pause for scrolling.

Administering the Wireless Device

This module describes the following wireless device administration tasks.

Securing Access to the Wireless Device

Administering the Access Point Hardware and Software

Administering Wireless Device Communication

Disabling the Mode Button Function

To disable the mode button on the wireless device, use the **[no] boot mode-button** command.

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

Note To reboot the wireless device, use the **service-module wlan-ap reset** command from the router's Cisco IOS CLI. See the "Rebooting the Wireless Device" section on page 12-20 for information about this command.

The mode button is enabled by default. To disable the access point's mode button, follow these steps, beginning in privileged EXEC mode:

SUMMARY STEPS

1. **configure terminal**
2. **no boot mode-button**
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**no boot mode-button**	Disables the access point's mode button.
Step 3	**end**	Returns to privileged EXEC mode. **Note** It is not necessary to save the configuration.

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

```
ap# show boot
BOOT path-list: flash:/c1200-k9w7-mx-v123_7_ja.20050430/c1200-k9w7-mx.v123_7_ja.20050430
Config file: flash:/config.txt
Private Config file: flash:/private-config
Enable Break: no
Manual boot:no
Mode button:on
Enable IOS break: no
HELPER path-list:
NVRAM/Config file
    buffer size: 32768

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

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

Preventing Unauthorized Access to Your Access Point

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

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

- Username and password pairs, which are locally stored on the wireless device. These pairs authenticate each user before the user can access the wireless device. You can also assign a specific privilege level (read only or read/write) to each username and password pair. For more information, see the "Configuring Username and Password Pairs" section on page 12-7. The default username is *Cisco*, and the default password is *Cisco*. Usernames and passwords are case sensitive.

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

- Username and password pairs are centrally stored in a database on a security server. For more information, see the "Controlling Access Point Access with RADIUS" section on page 12-10.

Protecting Access to Privileged EXEC Commands

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

Note For complete syntax and usage information for the commands used in this section, see *Cisco IOS Security Command Reference for Release 12.4*.

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

- Configuring Default Password and Privilege Level, page 12-4
- Setting or Changing a Static Enable Password, page 12-4
- Protecting Enable and Enable Secret Passwords with Encryption, page 12-5
- Configuring Username and Password Pairs, page 12-7
- Configuring Multiple Privilege Levels, page 12-8

Configuring Default Password and Privilege Level

Table 1 shows the default password and privilege level configuration.

Table 1 Default Passwords and Privilege Levels

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

Setting or Changing a Static Enable Password

The enable password controls access to the privileged EXEC mode.

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

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

SUMMARY STEPS

1. **configure terminal**
2. **enable password** *password*
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**enable password** *password*	Defines a new password or changes an existing password for access to privileged EXEC mode. • The default password is *Cisco*. • *password*—A string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. It can contain the question mark (?) character if you precede the question mark with the key combination Crtl-V when you create the password; for example, to create the password abc?123, do this: 1. Type **abc**. 2. Type **Crtl-V**. 3. Type **?123**. • When prompted to enter the enable password, you need not type Ctrl-V; you can simply enter **abc?123** at the password prompt. **Note** The characters TAB, ?, $, +, and [are invalid characters for passwords.
Step 3	**end**	Returns to privileged EXEC mode.
Step 4	**show running-config**	Verifies your entries.
Step 5	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

The enable password is not encrypted and can be read in the wireless device configuration file.

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

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

Protecting Enable and Enable Secret Passwords with Encryption

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

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

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

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

SUMMARY STEPS

1. **configure terminal**
2. **enable password** [**level** *level*] {*password* | *encryption-type encrypted-password*}
   or
   enable secret [**level** *level*] {*password* | *encryption-type encrypted-password*}
3. **service password-encryption**
4. **end**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.

Step 2	**enable password** [**level** *level*] {*password* | *encryption-type encrypted-password*}
	or
	enable secret [**level** *level*] {*password* | *encryption-type encrypted-password*}
		Defines a new password or changes an existing password for access to privileged EXEC mode.
		or
		Defines a secret password, which is saved using a nonreversible encryption method.
		• *level*—(Optional) Range is from 0 to 15. Level 1 is normal user EXEC mode privileges. The default level is 15 (privileged EXEC mode privileges).
		• *password*—A string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined.
		• *encryption-type*—(Optional) Only type 5. Cisco proprietary encryption algorithm, is available. If you specify an encryption type, you must provide an encrypted password—an encrypted password you copy from anotheraccess point wireless device configuration.
		Note If you specify an encryption type and then enter a clear text password, you cannot reenter privileged EXEC mode. You cannot recover a lost encrypted password by any method.

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

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

Use the **level** keyword to define a password for a specific privilege level. After you specify the level and set a password, give the password only to users who need to have access at this level. Use the **privilege level** command in global configuration mode to specify commands accessible at various levels. For more information, see the "Configuring Multiple Privilege Levels" section on page 12-8.

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

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

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

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

Configuring Username and Password Pairs

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

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

SUMMARY STEPS

1. **configure terminal**
2. **username** *name* [**privilege** *level*] {**password** *encryption-type password*}
3. **login local**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

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

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

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

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

Configuring Multiple Privilege Levels

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

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

This section includes this configuration information:

- Setting the Privilege Level for a Command, page 12-9
- Logging Into and Exiting a Privilege Level, page 12-10

Setting the Privilege Level for a Command

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

SUMMARY STEPS

1. **configure terminal**
2. **privilege** *mode* **level** *level command*
3. **enable password level** *level password*
4. **end**
5. **show running-config**
   or
   show privilege
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**privilege** *mode* **level** *level command*	Sets the privilege level for a command. • *mode*—Enter **configure** for global configuration mode, **exec** for EXEC mode, **interface** for interface configuration mode, or **line** for line configuration mode. • *level*—Range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. Level 15 is the level of access permitted by the **enable** password. • *command*—Specifies the command to which access is restricted.
Step 3	**enable password level** *level password*	Specifies the enable password for the privilege level. • *level*—Range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. • *password*—A string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined. **Note** The characters TAB, ?, $, +, and [are invalid characters for passwords.
Step 4	**end**	Returns to privileged EXEC mode.
Step 5	**show running-config** or **show privilege**	Verifies your entries. The **show running-config** command displays the password and access level configuration. The **show privilege** command displays the privilege level configuration.
Step 6	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

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

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

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

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

Logging Into and Exiting a Privilege Level

To log in to a specified privilege level or to exit to a specified privilege level, follow these steps, beginning in privileged EXEC mode:

SUMMARY STEPS

1. **enable** *level*
2. **disable** *level*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** *level*	Logs in to a specified privilege level. For *level*, the range is 0 to 15.
Step 2	**disable** *level*	Exits to a specified privilege level. For *level*, the range is 0 to 15.

Controlling Access Point Access with RADIUS

This section describes how to control administrator access to the wireless device by using Remote Authentication Dial-In User Service (RADIUS). For complete instructions on configuring the wireless device to support RADIUS, see the “Configuring Radius and TACACS+ Servers” chapter in *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.

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

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

These sections describe RADIUS configuration:

- Default RADIUS Configuration, page 12-11
- Configuring RADIUS Login Authentication, page 12-11 (required)
- Defining AAA Server Groups, page 12-13 (optional)
- Configuring RADIUS Authorization for User Privileged Access and Network Services, page 12-15 (optional)
- Displaying the RADIUS Configuration, page 12-16

Default RADIUS Configuration

RADIUS and AAA are disabled by default.

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

Configuring RADIUS Login Authentication

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

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

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

SUMMARY STEPS

1. **configure terminal**
2. **aaa new-model**
3. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
4. **line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]
5. **login authentication** {**default** | *list-name*}
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**aaa new-model**	Enables AAA.
Step 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	Creates a login authentication method list. • To create a default list that is used when a named list is *not* specified in the **login authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces. • *list-name*—A character string to name the list you are creating. • *method1...*—Specifies the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. Select one of these methods: • **local**—Use the local username database for authentication. You must enter username information in the database. Use the **username** *password* global configuration command. • **radius**—Use RADIUS authentication. You must configure the RADIUS server before you can use this authentication method. For more information, see the "Identifying the RADIUS Server Host" section of the "Configuring Radius and TACACS+ Servers" chapter in *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.
Step 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	Enters line configuration mode, and configures the lines to which the authentication list applies.
Step 5	**login authentication** {**default** | *list-name*}	Applies the authentication list to a line or set of lines. • If you specify **default**, use the default list that you created with the **aaa authentication login** command. • *list-name*—Specifies the list that you created with the **aaa authentication login** command.
Step 6	**end**	Returns to privileged EXEC mode.
Step 7	**show running-config**	Verifies your entries.
Step 8	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

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

Defining AAA Server Groups

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

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

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

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

SUMMARY STEPS

1. **configure terminal**
2. **aaa new-model**
3. **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]
4. **aaa group server radius** *group-name*
5. **server** *ip-address*
6. **end**
7. **show running-config**
8. **copy running-config startup-config**
9. Enable RADIUS login authentication

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**aaa new-model**	Enables AAA.

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

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

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

```
AP(config)# aaa new-model
AP(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
AP(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
AP(config)# aaa group server radius group1
AP(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
AP(config-sg-radius)# exit
AP(config)# aaa group server radius group2
AP(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
AP(config-sg-radius)# exit
```

Configuring RADIUS Authorization for User Privileged Access and Network Services

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

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

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

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

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

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

SUMMARY STEPS

1. **configure terminal**
2. **aaa authorization network radius**
3. **aaa authorization exec radius**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**aaa authorization network radius**	Configures the wireless device for user RADIUS authorization for all network-related service requests.
Step 3	**aaa authorization exec radius**	Configures the wireless device for user RADIUS authorization to determine whether the user has privileged EXEC access. The **exec** keyword might return user profile information (such as **autocommand** information).
Step 4	**end**	Returns to privileged EXEC mode.
Step 5	**show running-config**	Verifies your entries.
Step 6	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

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

Displaying the RADIUS Configuration

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

Controlling Access Point Access with TACACS+

This section describes how to control administrator access to the wireless device using Terminal Access Controller Access Control System Plus (TACACS+). For complete instructions on configuring the wireless device to support TACACS+, see the "Configuring Radius and TACACS+ Servers" chapter in *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.

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

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

These sections describe TACACS+ configuration:

- Default TACACS+ Configuration, page 12-17
- Configuring TACACS+ Login Authentication, page 12-17
- Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services, page 12-18
- Displaying the TACACS+ Configuration, page 12-19

Default TACACS+ Configuration

TACACS+ and AAA are disabled by default.

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

Configuring TACACS+ Login Authentication

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

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

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

SUMMARY STEPS

1. **configure terminal**
2. **aaa new-model**
3. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
4. **line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]
5. **login authentication** {**default** | *list-name*}
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**aaa new-model**	Enables AAA.

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

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

Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services

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

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

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

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

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

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

SUMMARY STEPS

1. **configure terminal**
2. **aaa authorization network tacacs+**
3. **aaa authorization exec tacacs+**
4. **end**
5. **show running-config**
6. **show running-config**

DETAILED STEPS

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

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

Displaying the TACACS+ Configuration

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

Administering the Wireless Hardware and Software

This section provides instructions for performing the following tasks:

- Resetting the Wireless Device to the Factory Default Configuration, page 12-20
- Rebooting the Wireless Device, page 12-20
- Monitoring the Wireless Device, page 12-20

Resetting the Wireless Device to the Factory Default Configuration

To reset the wireless device hardware and software to its factory default configuration, use the **service-module wlan-ap0 reset default-config** command in the router's Cisco IOS privileged EXEC mode.

Caution Because you may lose data, use only the **service-module wlan-ap0 reset** command to recover from a shutdown or failed state.

Rebooting the Wireless Device

To perform a graceful shutdown and reboot the wireless device, use the **service-module wlan-ap0 reload** command in the router's Cisco IOS privileged EXEC mode. At the confirmation prompt, press **Enter** to confirm the action, or enter **n** to cancel.

When running in autonomous mode, the reload command saves the configuration before rebooting. If the attempt is unsuccessful, the following message displays:

```
Failed to save service module configuration.
```

When running in Lightweight Access Point Protocol (LWAPP) mode, the reload function is typically handled by the wireless LAN controller (WLC). If you enter the **service-module wlan-ap0 reload** command, you will be prompted with the following message:

```
The AP is in LWAPP mode. Reload is normally handled by WLC controller.

Still want to proceed? [yes]
```

Monitoring the Wireless Device

This section provides commands for monitoring hardware on the router.

- Displaying Wireless Device Statistics, page 12-21
- Displaying Wireless Device Status, page 12-21

Displaying Wireless Device Statistics

Use the **service-module wlan-ap0 statistics** command in privileged EXEC mode to display wireless device statistics. The following is sample output for the command:

```
  CLI reset count = 0
  CLI reload count = 1
  Registration request timeout reset count = 0
  Error recovery timeout reset count = 0
  Module registration count = 10

The last IOS initiated event was a cli reload at *04:27:32.041 UTC Fri Mar 8 2007
```

Displaying Wireless Device Status

Use the **service-module wlan-ap0 status** command in privileged EXEC mode to display the status of the wireless device and its configuration information. The following is sample output for the command:

```
Service Module is Cisco wlan-ap0
Service Module supports session via TTY line 2
Service Module is in Steady state
Service Module reset on error is disabled
Getting status from the Service Module, please wait..

Image path = flash:c8xx_19xx_ap-k9w7-mx.acregr/c8xx_19xx_ap-k9w7-mx.acre
gr
System uptime = 0 days, 4 hours, 28 minutes, 5 seconds
Router#d was introduced for embedded wireless LAN access points on Integrated Services
Routers.
```

Managing the System Time and Date

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

Note For complete syntax and usage information for the commands used in this section, see *Cisco IOS Configuration Fundamentals Command Reference for Release 12.4*.

This section provides the following configuration information:

- Understanding Simple Network Time Protocol, page 12-21
- Configuring SNTP, page 12-22
- Configuring Time and Date Manually, page 12-22

Understanding Simple Network Time Protocol

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

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

http://www.cisco.com/en/US/docs/ios/12_1/configfun/configuration/guide/fcd303.html#wp1001075

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

Configuring SNTP

SNTP is disabled by default. To enable SNTP on the access point, use one or both of the commands listed in Table 2 in global configuration mode.

Table 2 SNTP Commands

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

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

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

Configuring Time and Date Manually

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

This section contains the following configuration information:

- Setting the System Clock, page 12-23
- Displaying the Time and Date Configuration, page 12-23
- Configuring the Time Zone, page 12-24
- Configuring Summer Time (Daylight Saving Time), page 12-24

Setting the System Clock

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

To set the system clock, follow these steps, beginning in privileged EXEC mode:

SUMMARY STEPS

1. **clock set** *hh***:***mm***:***ss day month year*
   or
   clock set *hh***:***mm***:***ss month day year*
2. **show running-config**
3. **copy running-config startup-config**

DETAILED STEPS

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

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

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

Displaying the Time and Date Configuration

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

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

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

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

Configuring the Time Zone

To manually configure the time zone, follow these steps, beginning in privileged EXEC mode:

SUMMARY STEPS

1. **configure terminal**
2. **clock timezone** *zone hours-offset* [*minutes-offset*]
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**clock timezone** *zone hours-offset* [*minutes-offset*]	Sets the time zone. **Note** The wireless device keeps internal time in universal time coordinated (UTC). Use this command only for display purposes and when the time is manually set. • *zone*—Enter the name of the time zone to be displayed when standard time is in effect. The default is UTC. • *hours-offset*—Enter the hours offset from UTC. • *minutes-offset*—(Optional) Enter the minutes offset from UTC.
Step 3	**end**	Returns to privileged EXEC mode.
Step 4	**show running-config**	Verifies your entries.
Step 5	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

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

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

Configuring Summer Time (Daylight Saving Time)

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

SUMMARY STEPS

1. **configure terminal**
2. **clock summer-time** *zone* **recurring** [*week day month hh***:***mm week day month hh***:***mm* [*offset*]]
3. **end**

4. **show running-config**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**clock summer-time** *zone* **recurring** [*week day month hh***:***mm week day month hh***:***mm* [*offset*]]	Configures summer time to start and end on the specified days every year. Summer time is disabled by default. If you specify **clock summer-time** *zone* **recurring** without parameters, the summer time rules default to the United States rules. • *zone*—Specifies the name of the time zone (for example, PDT) to be displayed when summer time is in effect. • *week*—(Optional) Specifies the week of the month (1 to 5 or **last**). • *day*—(Optional) Specifies the day of the week (for example, Sunday). • *month*—(Optional) Specifies the month (for example, January). • *hh***:***mm*—(Optional) Specifies the time (24-hour format) in hours and minutes. • *offset*—(Optional) Specifies the number of minutes to add during summer time. The default is 60.
Step 3	**end**	Returns to privileged EXEC mode.
Step 4	**show running-config**	Verifies your entries.
Step 5	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

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

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

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

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

SUMMARY STEPS

1. **configure terminal**
2. **clock summer-time** *zone* **date** [*month date year hh***:***mm month date year hh***:***mm* [*offset*]]
   or
   clock summer-time *zone* **date** [*date month year hh***:***mm date month year hh***:***mm* [*offset*]]
3. **end**
4. **show running-config**

5. **copy running-config startup-config**

DETAILED STEPS

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

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

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

This example shows how to set summer time to start on October 12, 2000, at 02:00, and end on April 26, 2001, at 02:00:

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

Configuring a System Name and Prompt

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

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

Note For complete syntax and usage information for the commands used in this section, see *Cisco IOS Configuration Fundamentals Command Reference* and *Cisco IOS IP Addressing Services Command Reference*.

This section contains the following configuration information:

- Default System Name and Prompt Configuration, page 12-27
- Configuring a System Name, page 12-27
- Understanding DNS, page 12-28

Default System Name and Prompt Configuration

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

Configuring a System Name

To manually configure a system name, follow these steps, beginning in privileged EXEC mode:

SUMMARY STEPS

1. **configure terminal**
2. **hostname** *name*
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**hostname** *name*	Manually configures a system name. The default setting is *ap*. **Note** When you change the system name, the wireless device radios are reset, and associated client devices disassociate and quickly reassociate. **Note** You can enter up to 63 characters for the system name. However, when the wireless device identifies itself to client devices, it uses only the first 15 characters in the system name. If it is important for client users to distinguish between devices, make sure that a unique portion of the system name appears in the first 15 characters.
Step 3	**end**	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 4	**show running-config**	Verifies your entries.
Step 5	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

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

To return to the default hostname, use the **no hostname** command in global configuration mode.

Understanding DNS

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

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

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

This section contains the following configuration information:

- Default DNS Configuration, page 12-28
- Setting Up DNS, page 12-28
- Displaying the DNS Configuration, page 12-30

Default DNS Configuration

Table 12-3 describes the default DNS configuration.

Table 12-3 Default DNS Configuration

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

Setting Up DNS

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

SUMMARY STEPS

1. **configure terminal**
2. **ip domain-name** *name*

3. **ip name-server** *server-address1* [*server-address2 ... server-address6*]
4. **ip domain-lookup**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

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

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

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

Displaying the DNS Configuration

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

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

Creating a Banner

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

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

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

This section contains the following configuration information:

- Default Banner Configuration, page 12-30
- Configuring a Message-of-the-Day Login Banner, page 12-31
- Configuring a Login Banner, page 12-32

Default Banner Configuration

The MOTD and login banners are not configured.

Configuring a Message-of-the-Day Login Banner

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

To configure an MOTD login banner, follow these steps, beginning in privileged EXEC mode:

SUMMARY STEPS

1. **configure terminal**
2. **banner motd** *c message c*
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

DETAILED STEPS

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

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

The following example shows how to configure a MOTD banner for the wireless device. The pound sign (#) is used as the beginning and ending delimiter:

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

This example shows the banner that results from the previous configuration:

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

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

```
User Access Verification

Password:
```

Configuring a Login Banner

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

To configure a login banner, follow these steps, beginning in privileged EXEC mode:

SUMMARY STEPS

1. **configure terminal**
2. **banner login** *c message c*
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

DETAILED STEPS

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

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

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

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

Configuring Ethernet Speed and Duplex Settings

The Cisco 1941-W ISR interface supports only 1000 Mbps speed and duplex settings by default, and the interface is always up. When the wireless device receives inline power from a switch, any change in the speed or duplex settings that resets the Ethernet link reboots the wireless device.

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

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

SUMMARY STEPS

1. **configure terminal**
2. **interface fastethernet0**
3. **speed** {**10** | **100** | **auto**}
4. **duplex** {**auto** | **full** | **half**}
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface fastethernet0**	Enters configuration interface mode.
Step 3	**speed** {**10** | **100** | **auto**}	Configures the Ethernet speed. **Note** We recommend that you use **auto**, the default setting.
Step 4	**duplex** {**auto** | **full** | **half**}	Configures the duplex setting. **Note** We recommend that you use **auto**, the default setting.
Step 5	**end**	Returns to privileged EXEC mode.
Step 6	**show running-config**	Verifies your entries.
Step 7	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Configuring the Access Point for Wireless Network Management

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

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

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

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

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

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

Configuring the Access Point for Local Authentication and Authorization

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

Note You can configure the wireless device as a local authenticator for 802.1x-enabled client devices to provide a backup for your main server or to provide authentication service on a network without a RADIUS server. See the *Using the Access Point as a Local Authenticator* document on Cisco.com for detailed instructions on configuring the wireless device as a local authenticator.

http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html

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

SUMMARY STEPS

1. **configure terminal**
2. **aaa new-model**
3. **aaa authentication login default local**
4. **aaa authorization exec local**
5. **aaa authorization network local**
6. **username** *name* [**privilege** *level*] {**password** *encryption-type password*}
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

DETAILED STEPS

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

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

Configuring the Authentication Cache and Profile

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

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

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

cache expiry
cache authorization profile
cache authentication profile
aaa cache profile

Note See *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges, Versions 12.4(10b)JA and 12.3(8)JEC* for information about these commands.

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

```
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
!
username Cisco password 7 123A0C041104
username admin privilege 15 password 7 01030717481C091D25
ip subnet-zero
!
!
aaa new-model
!
!
aaa group server radius rad_eap
server 192.168.134.229 auth-port 1645 acct-port 1646
!
aaa group server radius rad_mac
server 192.168.134.229 auth-port 1645 acct-port 1646
!
aaa group server radius rad_acct
server 192.168.134.229 auth-port 1645 acct-port 1646
!
aaa group server radius rad_admin
server 192.168.134.229 auth-port 1645 acct-port 1646
cache expiry 1
cache authorization profile admin_cache
cache authentication profile admin_cache
!
aaa group server tacacs+ tac_admin
server 192.168.133.231
cache expiry 1
cache authorization profile admin_cache
cache authentication profile admin_cache
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login default local cache tac_admin group tac_admin
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local cache tac_admin group tac_admin
aaa accounting network acct_methods start-stop group rad_acct
      aaa cache profile admin_cache
      all
      !
      aaa session-id common
      !
      !
      !
      bridge irb
      !
      !
      interface Dot11Radio0
      no ip address
      no ip route-cache
      shutdown
      speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
      station-role root
      bridge-group 1
      bridge-group 1 subscriber-loop-control
      bridge-group 1 block-unknown-source
      no bridge-group 1 source-learning
      no bridge-group 1 unicast-flooding
      bridge-group 1 spanning-disabled
      !
      interface Dot11Radio1
      no ip address
      no ip route-cache
      shutdown
      speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
      station-role root
      bridge-group 1
      bridge-group 1 subscriber-loop-control
      bridge-group 1 block-unknown-source
      no bridge-group 1 source-learning
      no bridge-group 1 unicast-flooding
      bridge-group 1 spanning-disabled
      !
      interface FastEthernet0
      no ip address
      no ip route-cache
      duplex auto
      speed auto
      bridge-group 1
      no bridge-group 1 source-learning
      bridge-group 1 spanning-disabled
      !
      interface BVI1
      ip address 192.168.133.207 255.255.255.0
      no ip route-cache
      !
      ip http server
      ip http authentication aaa
      no ip http secure-server
      ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
      ip radius source-interface BVI1
      !
      tacacs-server host 192.168.133.231 key 7 105E080A16001D1908
      tacacs-server directed-request
      radius-server attribute 32 include-in-access-req format %h
      radius-server host 192.168.134.229 auth-port 1645 acct-port 1646 key 7 111918160405041E00
      radius-server vsa send accounting
      !
      control-plane
      !
      bridge 1 route ip
```

```
!
!
!
line con 0
transport preferred all
transport output all
line vty 0 4
transport preferred all
transport input all
transport output all
line vty 5 15
transport preferred all
transport input all
transport output all
!
end
```

Configuring the Access Point to Provide DHCP Service

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

- Setting up the DHCP Server, page 12-38
- Monitoring and Maintaining the DHCP Server Access Point, page 12-40

Setting up the DHCP Server

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

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

For detailed information on DHCP-related commands and options, see the DHCP part in *Cisco IOS IP Addressing Services Configuration Guide, Release 12.4* at:

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_rdmp_ps6350_TSD_Products_Configuration_Guide_Chapter.html

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

SUMMARY STEPS

1. **configure terminal**
2. **ip dhcp excluded-address** *low_address* [*high_address*]
3. **ip dhcp pool** *pool_name*
4. **network** *subnet_number* [*mask* | *prefix-length*]
5. **lease** {*days* [*hours*] [*minutes*] | **infinite**}

6. **default-router** *address* [*address2 ... address 8*]
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `AP# configure terminal`	Enters global configuration mode.
Step 2	**ip dhcp excluded-address** *low_address* [*high_address*]	Excludes the wireless device IP address from the range of addresses that the wireless device assigns. • Enter the IP address in four groups of characters, such as 10.91.6.158. • The wireless device assumes that all IP addresses in a DHCP address pool subnet are available for assigning to DHCP clients. You must specify the IP addresses that the DHCP server should not assign to clients. • (Optional) To enter a range of excluded addresses, enter the address at the low end of the range, followed by the address at the high end of the range.
Step 3	**ip dhcp pool** *pool_name*	Creates a name for the pool of IP addresses that the wireless device assigns in response to DHCP requests, and enters DHCP configuration mode.
Step 4	**network** *subnet_number* [*mask* | *prefix-length*]	Assigns the subnet number for the address pool. The wireless device assigns IP addresses within this subnet. (Optional) Assigns a subnet mask for the address pool, or specifies the number of bits that compose the address prefix. The prefix is an alternative way of assigning the network mask. The prefix length must be preceded by a forward slash (/).
Step 5	**lease** {*days* [*hours*] [*minutes*] | **infinite**}	Configures the duration of the lease for IP addresses assigned by the wireless device. • *days*—Lease duration in number of days. • *hours*—(Optional) Lease duration in number of hours. • *minutes*—(Optional) Lease duration in number of minutes. • **infinite**—Sets the lease duration to infinite.
Step 6	**default-router** *address* [*address2 ... address 8*]	Specifies the IP address of the default router for DHCP clients on the subnet. **Note** One IP address is required; however, you can specify up to eight addresses in one command line.
Step 7	**end**	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 8	**show running-config**	Verifies your entries.
Step 9	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

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

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

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

Monitoring and Maintaining the DHCP Server Access Point

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

- show Commands, page 12-40
- clear Commands, page 12-41
- debug Command, page 12-41

show Commands

To display information about the wireless device as DHCP server, enter the commands in Table 12-4, in privileged EXEC mode.

Table 12-4 Show Commands for DHCP Server

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

clear Commands

To clear DHCP server variables, use the commands in Table 12-5, in privileged EXEC mode.

Table 12-5 Clear Commands for DHCP Server

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

debug Command

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

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

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

Configuring the Access Point for Secure Shell

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

Note For complete syntax and usage information for the commands used in this section, see the "Secure Shell Commands" section in the *Cisco IOS Security Command Reference for Release 12.4.*

Understanding SSH

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

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

- RADIUS (for more information, see the "Controlling Access Point Access with RADIUS" section on page 12-10)
- Local authentication and authorization (for more information, see the "Configuring the Access Point for Local Authentication and Authorization" section on page 12-34)

For more information about SSH, see Part 5, "Other Security Features" in the *Cisco IOS Security Configuration Guide for Release 12.4*.

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

Configuring SSH

Before configuring SSH, download the cryptographic software image from Cisco.com. For more information, see release notes for this release.

For information about configuring SSH and displaying SSH settings, see Part 6, “Other Security Features” in *Cisco IOS Security Configuration Guide for Release 12.4*, which is available at:

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4/sec_12_4_book.html

Configuring Client ARP Caching

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

This section contains this information:

- Understanding Client ARP Caching, page 12-42
- Configuring ARP Caching, page 12-43

Understanding Client ARP Caching

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

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

Optional ARP Caching

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

Configuring ARP Caching

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

SUMMARY STEPS

1. **configure terminal**
2. **dot11 arp-cache** [**optional**]
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

DETAILED STEPS

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

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

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

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

This feature modifies the way that point-to-multipoint bridging can be configured to operate on multiple VLANs with the ability to control traffic rates on each VLAN.

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

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

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

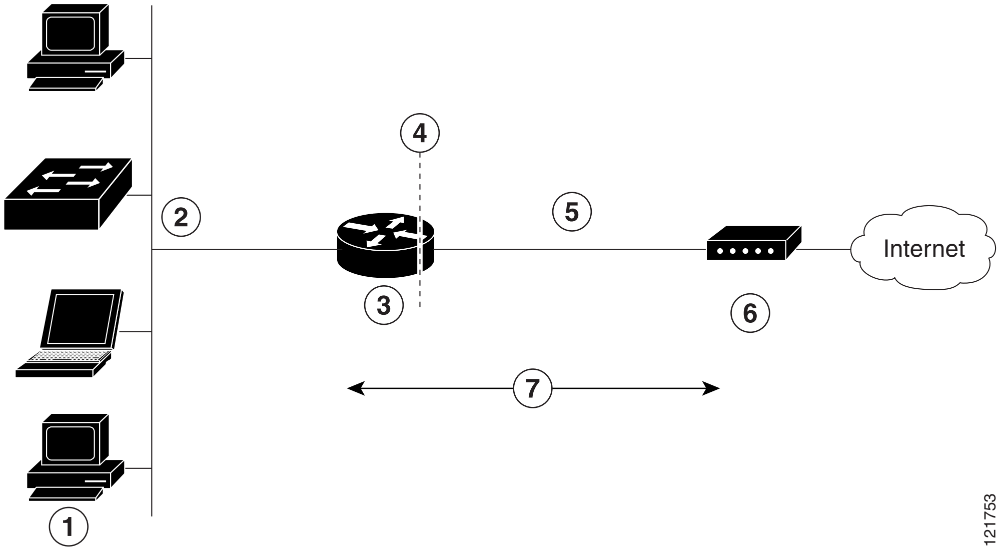
CHAPTER 13

Configuring PPP over Ethernet with NAT

This chapter provides an overview of Point-to-Point Protocol over Ethernet (PPPoE) clients and network address translation (NAT) that can be configured on the Cisco 860, Cisco 880, and Cisco 890 series Integrated Services Routers (ISRs).

Multiple PCs can be connected to the LAN behind the router. Before the traffic from these PCs is sent to the PPPoE session, it can be encrypted, filtered, and so forth. Figure 13-1 shows a typical deployment scenario with a PPPoE client and NAT configured on the Cisco router.

Figure 13-1 PPP over Ethernet with NAT



1	Multiple networked devices—Desktops, laptop PCs, switches
2	Fast Ethernet LAN interface (inside interface for NAT)
3	PPPoE client—Cisco 860, Cisco 880, or Cisco 890 ISRs
4	Point at which NAT occurs
5	Fast Ethernet WAN interface (outside interface for NAT)
6	Cable modem or other server that is connected to the Internet
7	PPPoE session between the client and a PPPoE server

PPPoE

The PPPoE client feature on the router provides PPPoE client support on Ethernet interfaces. A dialer interface must be used for cloning virtual access. Multiple PPPoE client sessions can be configured on an Ethernet interface, but each session must use a separate dialer interface and a separate dialer pool.

A PPPoE session is initiated on the client side by the Cisco 860 or Cisco 880 ISRs. An established PPPoE client session can be terminated in one of two ways:

- By entering the **clear vpdn tunnel pppoe** command. The PPPoE client session is terminated, and the PPPoE client immediately tries to reestablish the session. This also occurs if the session has a timeout.
- By entering the **no pppoe-client dial-pool** *number* command to clear the session. The PPPoE client does not attempt to reestablish the session.

NAT

NAT (represented as the dashed line at the edge of the Cisco router) signifies two addressing domains and the inside source address. The source list defines how the packet travels through the network.

Configuration Tasks

Perform the following tasks to configure this network scenario:

- Configure the Virtual Private Dialup Network Group Number
- Configure Ethernet WAN Interfaces
- Configure the Dialer Interface
- Configure Network Address Translation

An example showing the results of these configuration tasks is shown in the "Configuration Example" section on page 13-9.

Configure the Virtual Private Dialup Network Group Number

Configuring a virtual private dialup network (VPDN) enables multiple clients to communicate through the router by way of a single IP address.

To configure a VPDN, perform the following steps, starting in global configuration mode:

SUMMARY STEPS

1. **vpdn enable**
2. **vpdn-group** *name*
3. **request-dialin**
4. **protocol** {**l2tp** | **pppoe**}
5. **exit**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**vpdn enable** **Example:** `Router(config)# vpdn enable`	Enables VPDN on the router.
Step 2	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group 1`	Creates and associates a VPDN group with a customer or VPDN profile.
Step 3	**request-dialin** **Example:** `Router(config-vpdn)# request-dialin`	Creates a request-dialin VPDN subgroup, indicating the dialing direction, and initiates the tunnel.

Step 4	**protocol** {**l2tp** | **pppoe**}
	Example:
	`Router(config-vpdn-req-in)# protocol pppoe`
		Specifies the type of sessions the VPDN subgroup can establish.

Step 5	**exit** **Example:** `Router(config-vpdn-req-in)# exit`	Exits request-dialin VPDN group configuration mode.
Step 6	**exit** **Example:** `Router(config-vpdn)# exit`	Exits VPDN configuration mode and returns to global configuration mode.

Configure Ethernet WAN Interfaces

In this scenario, the PPPoE client (your Cisco router) communicates over a 10/100/1000 Mbps-Ethernet interface on both the inside and the outside.

To configure the Fast Ethernet WAN interfaces, perform these steps, starting in global configuration mode:

SUMMARY STEPS

1. **interface** *type number*
2. **pppoe-client dial-pool-number** *number*
3. **no shutdown**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**interface** *type number*
	Example:
	`Router(config)# interface fastethernet 4`
	`OR`
	`Router(config)# interface gigabitethernet 4`
		Enters interface configuration mode for the WAN interface.

Step 2	**pppoe-client dial-pool-number** *number* **Example:** `Router(config-if)# pppoe-client dial-pool-number 1`	Configures the PPPoE client and specifies the dialer interface to use for cloning.
Step 3	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the Fast Ethernet interface and the configuration changes just made to it.
Step 4	**exit** **Example:** `Router(config-if)# exit`	Exits configuration mode for the Fast Ethernet interface and returns to global configuration mode.

Ethernet Operations, Administration, and Maintenance

Ethernet Operations, Administration, and Maintenance (OAM) is a protocol for installing, monitoring, and troubleshooting Ethernet metropolitan-area networks (MANs) and Ethernet WANs. It relies on a new, optional sublayer in the data link layer of the Open Systems Interconnection (OSI) model. The OAM features covered by this protocol are Discovery, Link Monitoring, Remote Fault Detection, Remote Loopback, and Cisco Proprietary Extensions.

For setup and configuration information about Ethernet OAM, see *Using Ethernet Operations, Administration, and Maintenance* at:

http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_oam_ps10591_TSD_Products_Configuration_Guide_Chapter.html.

Configure the Dialer Interface

The dialer interface indicates how to handle traffic from the clients, including, for example, default routing information, the encapsulation protocol, and the dialer pool to use. The dialer interface is also used for cloning virtual access. Multiple PPPoE client sessions can be configured on a Fast Ethernet interface, but each session must use a separate dialer interface and a separate dialer pool.

To configure a dialer interface for one of the Fast Ethernet LAN interfaces on the router, complete the following steps, starting in global configuration mode:

SUMMARY STEPS

1. **interface dialer** *dialer-rotary-group-number*
2. **ip address negotiated**
3. **ip mtu** *bytes*
4. **encapsulation** *encapsulation-type*
5. **ppp authentication** {*protocol1* [*protocol2...*]}
6. **dialer pool** *number*
7. **dialer-group** *group-number*
8. **exit**
9. **dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | **access-group**}
10. **ip route** *prefix mask* {*interface-type interface-number*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface dialer** *dialer-rotary-group-number* **Example:** `Router(config)# interface dialer 0`	Creates a dialer interface and enters interface configuration mode. • Range is from 0 to 255.
Step 2	**ip address negotiated** **Example:** `Router(config-if)# ip address negotiated`	Specifies that the IP address for the interface is obtained through PPP/IPCP (IP Control Protocol) address negotiation.
Step 3	**ip mtu** *bytes* **Example:** `Router(config-if)# ip mtu 1492`	Sets the size of the IP maximum transmission unit (MTU). • The default minimum is 128 bytes. The maximum for Ethernet is 1492 bytes.
Step 4	**encapsulation** *encapsulation-type* **Example:** `Router(config-if)# encapsulation ppp`	Sets the encapsulation type to PPP for the data packets being transmitted and received.

	Command or Action	Purpose

Step 5	**ppp authentication** {*protocol1* [*protocol2...*]}
	Example:
	`Router(config-if)# ppp authentication chap`
		Sets the PPP authentication method to Challenge Handshake Authentication Protocol (CHAP).
		For details about this command and additional parameters that can be set, see *Cisco IOS Security Command Reference*.

Step 6	**dialer pool** *number* **Example:** `Router(config-if)# dialer pool 1`	Specifies the dialer pool that is used to connect to a specific destination subnetwork.
Step 7	**dialer-group** *group-number* **Example:** `Router(config-if)# dialer-group 1`	Assigns the dialer interface to a dialer group. • Range is from 1 to 10. **Tip** Using a dialer group controls access to your router.
Step 8	**exit** **Example:** `Router(config-if)# exit`	Exits the dialer 0 interface configuration mode and returns to global configuration mode.

Step 9	**dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | **access-group**}
	Example:
	`Router(config)# dialer-list 1 protocol ip permit`
		Creates a dialer list and associates a dial group with it. Packets are then forwarded through the specified interface dialer group.
		For details about this command and additional parameters that can be set, see *Cisco IOS Dial Technologies Command Reference*.

Step 10	**ip route** *prefix mask* {*interface-type interface-number*}
	Example:
	`Router(config)# ip route 10.10.25.2 255.255.255.255 dialer 0`
		Sets the IP route for the default gateway for the dialer 0 interface.
		For details about this command and additional parameters that can be set, see *Cisco IOS IP Command Reference, Volume 2; Routing Protocols*.

Configure Network Address Translation

Network Address Translation (NAT) translates packets from addresses that match a standard access list, using global addresses allocated by the dialer interface. Packets that enter the router through the inside interface, packets sourced from the router, or both are checked against the access list for possible address translation. You can configure NAT for either static or dynamic address translations.

To configure the outside Fast Ethernet WAN interface with dynamic NAT, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}
2. **ip nat inside source** {**list** *access-list-number*} {**interface** *type number* | **pool** *name*} [**overload**]
3. **interface** *type number*

4. **ip nat** {**inside** | **outside**}
5. **no shutdown**
6. **exit**
7. **interface** *type number*
8. **ip nat** {**inside** | **outside**}
9. **no shutdown**
10. **exit**
11. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]

DETAILED STEPS

	Command or Action	Purpose

Step 1	**ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}
	Example:
	`Router(config)# ip nat pool pool1 192.168.1.0 192.168.2.0 netmask 255.255.252.0`
		Creates pool of global IP addresses for NAT.

Step 2	**ip nat inside source** {**list** *access-list-number*} {**interface** *type number* | **pool** *name*} [**overload**]
	Example:
	`Router(config)# ip nat inside source list 1 interface dialer 0 overload`
	`or`
	`Router(config)# ip nat inside source list acl1 pool pool1`
		Enables dynamic translation of addresses on the inside interface.
		The first example shows the addresses permitted by the access list *1* to be translated to one of the addresses specified in the dialer interface *0*.
		The second example shows the addresses permitted by access list *acl1* to be translated to one of the addresses specified in the NAT pool *pool1*.
		For details about this command and additional parameters that can be set, as well as information about enabling static translation, see *Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services*.

Step 3	**interface** *type number* **Example:** `Router(config)# interface vlan 1`	Enters configuration mode for the VLAN (on which the Fast Ethernet LAN interfaces [FE0–FE3] reside) to be the inside interface for NAT.

Step 4	**ip nat** {**inside** | **outside**}
	Example:
	`Router(config-if)# ip nat inside`
		Identifies the specified VLAN interface as the NAT inside interface.
		For details about this command and additional parameters that can be set, as well as information about enabling static translation, see *Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services*.

	Command or Action	Purpose
Step 5	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the configuration changes just made to the Ethernet interface.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits configuration mode for the Fast Ethernet interface and returns to global configuration mode.
Step 7	**interface** *type number* **Example:** `Router(config)# interface fastethernet 4`	Enters configuration mode for the Fast Ethernet WAN interface (FE4) to be the outside interface for NAT.

Step 8	**ip nat** {**inside** | **outside**}
	Example:
	`Router(config-if)# ip nat outside`
		Identifies the specified WAN interface as the NAT outside interface.
		For details about this command and additional parameters that can be set, as well as information about enabling static translation, see *Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services*.

Step 9	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the configuration changes just made to the Ethernet interface.
Step 10	**exit** **Example:** `Router(config-if)# exit`	Exits configuration mode for the Fast Ethernet interface and returns to global configuration mode.
Step 11	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] **Example:** `Router(config)# access-list 1 permit 192.168.1.0 255.255.255.0`	Defines a standard access list indicating which addresses need translation. **Note** All other addresses are implicitly denied.

Note To use NAT with a virtual-template interface, you must configure a loopback interface. See Chapter 3, "Basic Router Configuration," for information on configuring a loopback interface.

For complete information on the NAT commands, see the Cisco NX-OS Release 4.1 documentation set. For more general information on NAT concepts, see Appendix A, "Cisco IOS Software Basic Skills."

Configuration Example

The following configuration example shows a portion of the configuration file for the PPPoE scenario described in this chapter.

The VLAN interface has an IP address of 192.168.1.1 with a subnet mask of 255.255.255.0. NAT is configured for inside and outside

Note Commands marked by “**(default)**” are generated automatically when you run the **show running-config** command.

```
vpdn enable
vpdn-group 1
request-dialin
protocol pppoe
!
interface vlan 1
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast (default)
ip nat inside
interface FastEthernet 4
no ip address
no ip directed-broadcast (default)
ip nat outside
pppoe enable group global
pppoe-client dial-pool-number 1
no sh
!
interface dialer 0
ip address negotiated
ip mtu 1492
encapsulation ppp
ppp authentication chap
dialer pool 1
dialer-group 1
!
dialer-list 1 protocol ip permit
ip nat inside source list 1 interface dialer 0 overload
ip classless (default)
ip route 10.10.25.2 255.255.255.255 dialer 0
ip nat pool pool1 192.168.1.0 192.168.2.0 netmask 255.255.252.0
ip nat inside source list acl1 pool pool1
!
```

Verifying Your Configuration

Use the **show ip nat statistics** command in privileged EXEC mode to verify the PPPoE with NAT configuration. You should see verification output similar to the following example:

```
Router# show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
  FastEthernet4
Inside interfaces:
  Vlan1
Hits: 0  Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
```

```
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 interface Dialer0 refcount 0
Queued Packets: 0
```

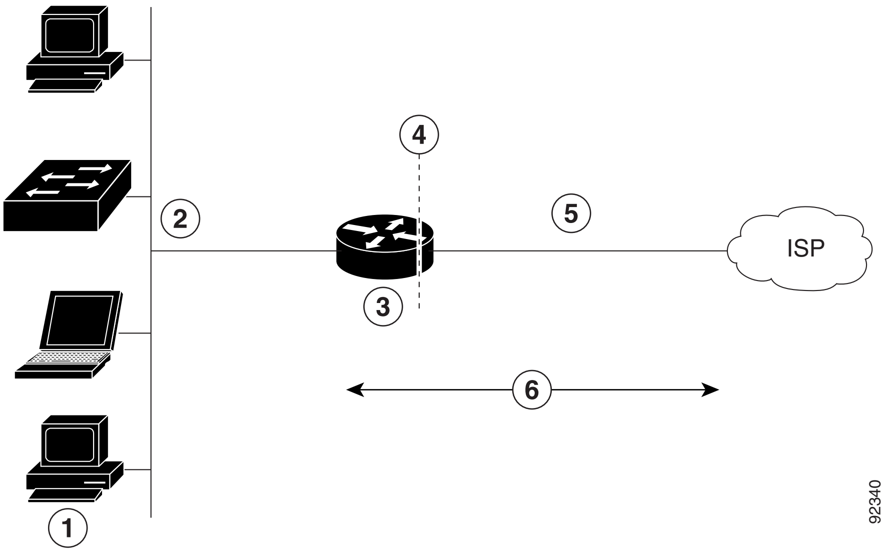
CHAPTER 14

Configuring PPP over ATM with NAT

This chapter provides an overview of Point-to-Point Protocol over Asynchronous Transfer Mode (PPPoA) clients and network address translation (NAT) that can be configured on the Cisco 860 and Cisco 880 series Integrated Services Routers (ISRs).

Multiple PCs can be connected to the LAN behind the router. Before traffic from the PCs is sent to the PPPoA session, it can be encrypted, filtered, and so forth. PPP over ATM provides a network solution with simplified address handling and straight user verification like a dial network. Figure 14-1 shows a typical deployment scenario with a PPPoA client and NAT configured on the Cisco router. This scenario uses a single static IP address for the ATM connection.

Figure 14-1 PPP over ATM with NAT



1	Small business with multiple networked devices—desktops, laptop PCs, switches
2	Fast Ethernet LAN interface (inside interface for NAT, 192.168.1.1/24)
3	PPPoA Client
4	Point at which NAT occurs
5	ATM WAN interface (outside interface for NAT)
6	PPPoA session between the client and a PPPoA server at the ISP

In this scenario, the small business or remote user on the Fast Ethernet LAN can connect to an Internet service provider (ISP) using the integrated xDSL WAN interface on the Cisco 860 and Cisco 880 series ISRs.

The Fast Ethernet interface carries the data packet through the LAN and off-loads it to the PPP connection on the ATM interface. The ATM traffic is encapsulated and sent over the xDSL interface. The dialer interface is used to connect to the ISP.

PPPoA

The PPPoA Client feature on the router provides PPPoA client support on ATM interfaces. A dialer interface must be used for cloning virtual access. Multiple PPPoA client sessions can be configured on an ATM interface, but each session must use a separate dialer interface and a separate dialer pool.

A PPPoA session is initiated on the client side by the Cisco 860 or Cisco 880 series router.

NAT

NAT (represented as the dashed line at the edge of the Cisco router) signifies two addressing domains and the inside source address. The source list defines how the packet travels through the network.

Configuration Tasks

Perform the following tasks to configure this network scenario:

- Configure the Dialer Interface
- Configure the ATM WAN Interface
- Configure DSL Signaling Protocol
- Configure Network Address Translation

An example showing the results of these configuration tasks is shown in the "Configuration Example" section on page 14-8.

Configure the Dialer Interface

The dialer interface indicates how to handle traffic from the clients, including, for example, default routing information, the encapsulation protocol, and the dialer pool to use. It is also used for cloning virtual access. Multiple PPPoA client sessions can be configured on an ATM interface, but each session must use a separate dialer interface and a separate dialer pool.

Perform these steps to configure a dialer interface for the ATM interface on the router, starting in global configuration mode.

	Command	Purpose
Step 1	**interface dialer** *dialer-rotary-group-number* **Example:** `Router(config)# interface dialer 0`	Creates a dialer interface (numbered 0–255), and enters into interface configuration mode.
Step 2	**ip address negotiated** **Example:** `Router(config-if)# ip address negotiated`	Specifies that the IP address for the dialer interface is obtained through PPP/IPCP (IP Control Protocol) address negotiation.

	Command	Purpose
Step 3	**ip mtu** *bytes* **Example:** `Router(config-if)# ip mtu 4470`	Sets the size of the IP maximum transmission unit (MTU). The default minimum is 128 bytes. The maximum for ATM is 4470 bytes.
Step 4	**encapsulation** *encapsulation-type* **Example:** `Router(config-if)# encapsulation ppp`	Sets the encapsulation type to PPP for the data packets being transmitted and received.

Step 5	**ppp authentication** {*protocol1* [*protocol2...*]}
	Example:
	`Router(config-if)# ppp authentication chap`
		Sets the PPP authentication method.
		The example applies the Challenge Handshake Authentication Protocol (CHAP).
		For details about this command and additional parameters that can be set, see the *Cisco IOS Security Command Reference.*

Step 6	**dialer pool** *number* **Example:** `Router(config-if)# dialer pool 1`	Specifies the dialer pool to use to connect to a specific destination subnetwork.
Step 7	**dialer-group** *group-number* **Example:** `Router(config-if)# dialer-group 1`	Assigns the dialer interface to a dialer group (1–10). **Tip** Using a dialer group controls access to your router.
Step 8	**exit** **Example:** `Router(config-if)# exit`	Exits the dialer 0 interface configuration.

Step 9	**dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | **access-group**}
	Example:
	`Router(config)# dialer-list 1 protocol ip permit`
		Creates a dialer list and associates a dial group with it. Packets are then forwarded through the specified interface dialer group.
		For details about this command and additional parameters that can be set, see the *Cisco IOS Dial Technologies Command Reference*.

Step 10	**ip route** *prefix mask* {*interface-type interface-number*}
	Example:
	`Router(config)# ip route 10.10.25.2 0.255.255.255 dialer 0`
		Sets the IP route for the default gateway for the dialer 0 interface.
		For details about this command and additional parameters that can be set, see the *Cisco IOS IP Command Reference, Volume 1 of 4: Routing Protocols*.

Repeat these steps for any additional dialer interfaces or dialer pools needed.

Configure the ATM WAN Interface

Perform these steps to configure the ATM interface, beginning in global configuration mode.

	Command	Purpose
Step 1	**interface** *type number* **Example:** `Router(config)# interface atm 0`	Enters interface configuration mode for the ATM interface (labeled ADSLoPOTS or G.SHDSL on the back of your router). **Note** This interface was initially configured during basic router configuration. See the "Configuring WAN Interfaces" section on page 3-8.
Step 2	**pvc** *vpi*/*vci* **Example:** `Router(config-if)# pvc 8/35`	Creates an ATM PVC for each end node (up to ten) with which the router communicates. Enters ATM virtual circuit configuration mode. When a PVC is defined, AAL5SNAP encapsulation is defined by default. Use the **encapsulation** command to change this, as shown in Step 3. The VPI and VCI arguments cannot be simultaneously specified as zero; if one is 0, the other cannot be 0. For details about this command and additional parameters that can be set, see the *Cisco IOS Wide-Area Networking Command Reference*.

Step 3	**encapsulation** {**aal5auto** | **aal5autoppp virtual-template** *number* [**group** *group-name*] | **aal5ciscoppp virtual-template** *number* | **aal5mux** *protocol* | **aal5nlpid** | **aal5snap**}
	Example:
	`Router(config-if-atm-vc)# encapsulation aal5mux ppp dialer`
		Specifies the encapsulation type for the PVC and points back to the dialer interface.
		For details about this command and additional parameters that can be set, see the *Cisco IOS Wide-Area Networking Command Reference*.

Step 4	**dialer pool-member** *number* **Example:** `Router(config-if-atm-vc)# dialer pool-member 1`	Specifies the ATM interface as a member of a dialer profile dialing pool. The pool number must be in the range of 1–255.
Step 5	**no shutdown** **Example:** `Router(config-if-atm-vc)# no shutdown`	Enables interface and configuration changes just made to the ATM interface.

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

Configure DSL Signaling Protocol

DSL signaling must be configured on the ATM interface for connection to your ISP. The Cisco 887 and Cisco 867 ISRs support ADSL signaling over POTS and the Cisco 886 ISR supports ADSL signaling over ISDN. The Cisco 888 ISR supports G.SHDSL.

Configuring ADSL

The default configuration for ADSL signaling is shown in Table 14-1.

Table 14-1 Default ADSL Configuration

Attribute	Description	Default Value
Operating mode	Specifies the operating mode of the digital subscriber line (DSL) for an ATM interface. • ADSL over POTS—ANSI or ITU full rate, or automatic selection. • ADSL over ISDN—ITU full rate, ETSI, or automatic selection.	Auto
Loss of margin	Specifies the number of times a loss of margin may occur.	—
Training log	Toggles between enabling the training log and disabling the training log.	Disabled

If you wish to change any of these settings, use one of the following commands in global configuration mode.

- **dsl operating-mode** (from the ATM interface configuration mode)
- **dsl lom** *integer*
- **dsl enable-training-log**

See the *Cisco IOS Wide-Area Networking Command Reference* for details of these commands.

Verify the Configuration

You can verify that the configuration is set the way you want by using the **show dsl interface atm** command from privileged EXEC mode.

```
Router# show dsl interface atm 0
ATM0
Alcatel 20190 chipset information
                ATU-R (DS)                      ATU-C (US)
Modem Status:    Showtime (DMTDSL_SHOWTIME)
DSL Mode:        ITU G.992.5 (ADSL2+) Annex A
ITU STD NUM:     0x03                            0x2
Chip Vendor ID:  'STMI'                          'BDCM'
Chip Vendor Specific:  0x0000                    0x6193
Chip Vendor Country:   0x0F                      0xB5
Modem Vendor ID: 'CSCO'                          '    '
Modem Vendor Specific: 0x0000                    0x0000
Modem Vendor Country:  0xB5                      0x00
Serial Number Near:
Serial Number Far:
```

```
Modem VerChip ID:        C196 (3)
DFE BOM:         DFE3.0 Annex A (1)
Capacity Used:   82%                             99%
Noise Margin:    12.5 dB                          5.5 dB
Output Power:    11.5 dBm                        12.0 dBm
Attenuation:      5.5 dB                          0.0 dB
FEC ES Errors:    0                               0
ES Errors:        1                              287
SES Errors:       1                               0
LOSES Errors:     1                               0
UES Errors:       0                              276233
Defect Status:   None                            None
Last Fail Code:  None
Watchdog Counter: 0x56
Watchdog Resets: 0
Selftest Result: 0x00
Subfunction:     0x00
Interrupts:      4147 (0 spurious)
PHY Access Err:  0
Activations:     3
LED Status:      ON
LED On Time:     100
LED Off Time:    100
Init FW:         init_AMR-4.0.015_no_bist.bin
Operation FW:    AMR-4.0.015.bin
FW Source:       embedded
FW Version:      4.0.15

                 DS Channel1      DS Channel0   US Channel1       US Channel0
Speed (kbps):             0            19999             0              1192
Cells:                    0                0             0           1680867
Reed-Solomon EC:          0                0             0                 0
CRC Errors:               0                0             0               326
Header Errors:            0                0             0               131
Total BER:                0E-0           65535E-0
Leakage Average BER:      0E-0           65535E-255
Interleave Delay:         0               36             0                11
                        ATU-R (DS)      ATU-C (US)
Bitswap:               enabled            enabled
Bitswap success:          0                  0
Bitswap failure:          0                  0

LOM Monitoring : Disabled


DMT Bits Per Bin
000: 0 0 0 0 F F F F F F F F F F F F
010: 0 0 3 0 F F F F F F F F F F F F
020: F F F F F F F F F F F F F F F F
....
DSL: Training log buffer capability is not enabled
Router#
```

Configure Network Address Translation

Network Address Translation (NAT) translates packets from addresses that match a standard access list, using global addresses allocated by the dialer interface. Packets that enter the router through the inside interface, packets sourced from the router, or both are checked against the access list for possible address translation. You can configure NAT for either static or dynamic address translations.

Perform these steps to configure the outside ATM WAN interface with dynamic NAT, beginning in global configuration mode:

	Command	Purpose

Step 1	**ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}
	Example:
	`Router(config)# ip nat pool pool1 192.168.1.0 192.168.2.0 netmask 255.255.255.0`
		Creates pool of global IP addresses for NAT.

Step 2	**ip nat inside source** {**list** *access-list-number*} {**interface** *type number* | **pool** *name*} [**overload**]
	Example 1:
	`Router(config)# ip nat inside source list 1 interface dialer 0 overload`
	or
	Example 2:
	`Router(config)# ip nat inside source list acl1 pool pool1`
		Enables dynamic translation of addresses on the inside interface.
		The first example shows the addresses permitted by the access list *1* to be translated to one of the addresses specified in the dialer interface *0*.
		The second example shows the addresses permitted by access list *acl1* to be translated to one of the addresses specified in the NAT pool *pool1*.
		For details about this command and additional parameters that can be set, as well as information about enabling static translation, see the *Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services*.

Step 3	**interface** *type number* **Example:** `Router(config)# interface vlan 1`	Enters configuration mode for the VLAN (on which the Fast Ethernet LAN interfaces [FE0–FE3] reside) to be the inside interface for NAT.

Step 4	**ip nat** {**inside** | **outside**}
	Example:
	`Router(config-if)# ip nat inside`
		Applies NAT to the Fast Ethernet LAN interface as the inside interface.
		For details about this command and additional parameters that can be set, as well as information about enabling static translation, see the *Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services*.

Step 5	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the configuration changes just made to the Ethernet interface.

	Command	Purpose
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits configuration mode for the Fast Ethernet interface.
Step 7	**interface** *type number* **Example:** `Router(config)# interface atm 0`	Enters configuration mode for the ATM WAN interface (ATM0) to be the outside interface for NAT.

Step 8	**ip nat** {**inside** | **outside**}
	Example:
	`Router(config-if)# ip nat outside`
		Identifies the specified WAN interface as the NAT outside interface.
		For details about this command and additional parameters that can be set, as well as enabling static translation, see the *Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services*.

Step 9	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the configuration changes just made to the Ethernet interface.
Step 10	**exit** **Example:** `Router(config-if)# exit`	Exits configuration mode for the ATM interface.
Step 11	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] **Example:** `Router(config)# access-list 1 permit 192.168.1.0 255.255.255.0`	Defines a standard access list permitting addresses that need translation. **Note** All other addresses are implicitly denied.

Note If you want to use NAT with a virtual-template interface, you must configure a loopback interface. See Chapter 3, "Basic Router Configuration," for information on configuring the loopback interface.

For complete information on NAT commands, see the Cisco NX-OS Release 4.1 documentation set.

Configuration Example

The following configuration example shows a portion of the configuration file for a client in the PPPoA scenario described in this chapter.

The VLAN interface has an IP address of 192.168.1.1 with a subnet mask of 255.255.255.0. NAT is configured for inside and outside.

Note Commands marked by "**(default)**" are generated automatically when you run the **show running-config** command.

```
!
interface Vlan1
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly (default)
!
interface ATM0
 no ip address
 ip nat outside
 ip virtual-reassembly
 no atm ilmi-keepalive
 pvc 8/35
  encapsulation aal5mux ppp dialer
  dialer pool-member 1
 !
 dsl operating-mode auto
!
interface Dialer0
 ip address negotiated
 ip mtu 1492
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 ppp authentication chap
!
ip classless (default)
!
ip nat pool pool1 192.168.1.0 192.168.2.0 netmask 0.0.0.255
ip nat inside source list 1 interface Dialer0 overload
!
access-list 1 permit 192.168.1.0 0.0.0.255
dialer-list 1 protocol ip permit

ip route 10.10.25.2 0.255.255.255 dialer 0
!
```

Verifying Your Configuration

Use the **show ip nat statistics** command in privileged EXEC mode to verify the PPPoA client with NAT configuration. You should see verification output similar to the following example:

```
Router# show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
  ATM0
Inside interfaces:
  Vlan1
Hits: 0  Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 interface Dialer0 refcount 0
Queued Packets: 0
```

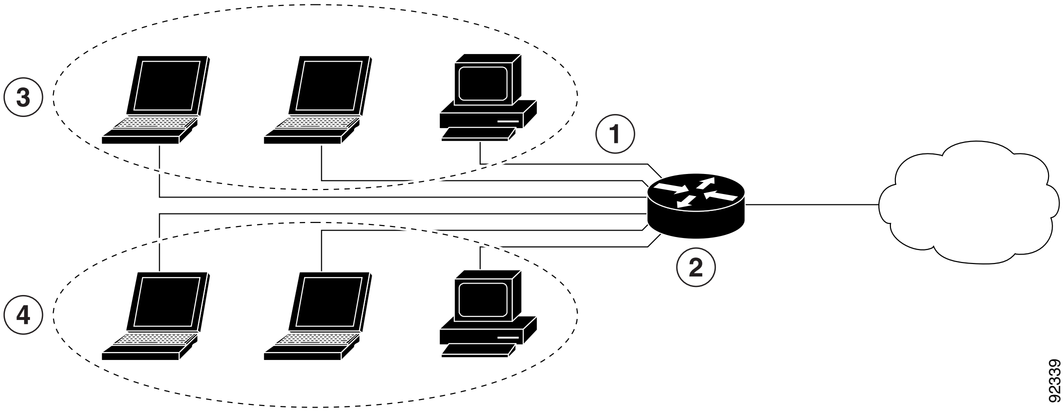
CHAPTER 13

Configuring a LAN with DHCP and VLANs

The Cisco 860 and Cisco 880 series Integrated Services Routers (ISRs) support clients on both physical LANs and VLANs. The routers can use the Dynamic Host Configuration Protocol (DHCP) to enable automatic assignment of IP configurations for nodes on these networks.

Figure 13-1 shows a typical deployment scenario with two physical LANs connected by the router and two VLANs.

Figure 13-1 Physical and Virtual LANs with DHCP Configured on the Cisco Router



1	Fast Ethernet LAN (with multiple networked devices)
2	Router and DHCP server—Cisco 860 and 880 series access router—connected to the Internet
3	VLAN 1
4	VLAN 2

DHCP

DHCP, which is described in RFC 2131, uses a client/server model for address allocation. As an administrator, you can configure your Cisco 800 series router to act as a DHCP server, providing IP address assignment and other TCP/IP-oriented configuration information to your workstations. DHCP frees you from having to manually assign an IP address to each client.

When you configure a DHCP server, you must configure the server properties, policies, and DHCP options.

Note Whenever you change server properties, you must reload the server with the configuration data from the Network Registrar database.

VLANs

The Cisco 860 and 880 series access routers support four Fast Ethernet ports on which you can configure VLANs.

VLANs enable networks to be segmented and formed into logical groups of users, regardless of the user's physical location or LAN connection.

Configuration Tasks

Perform the following tasks to configure this network scenario:

- Configure DHCP
- Configure VLANs

Note The procedures in this chapter assume you have already configured basic router features as well as PPPoE or PPPoA with NAT. If you have not performed these configurations tasks, see Chapter 3, "Basic Router Configuration," Chapter 13, "Configuring PPP over Ethernet with NAT," and Chapter 14, "Configuring PPP over ATM with NAT" as appropriate for your router.

Configure DHCP

To configure your router for DHCP operation, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **ip domain name** *name*
2. **ip name-server** *server-address1* [*server-address2*...*server-address6*]
3. **ip dhcp excluded-address** *low-address* [*high-address*]
4. **ip dhcp pool** *name*
5. **network** *network-number* [*mask* | *prefix-length*]
6. **import all**
7. **default-router** *address* [*address2*...*address8*]
8. **dns-server** *address* [*address2*...*address8*]
9. **domain-name** *domain*
10. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**ip domain name** *name*
	Example:
	`Router(config)# ip domain name smallbiz.com`
	`Router(config)#`
		Identifies the default domain that the router uses to complete unqualified hostnames (names without a dotted-decimal domain name).

Step 2	**ip name-server** *server-address1* [*server-address2...server-address6*]
	Example:
	`Router(config)# ip name-server 192.168.11.12`
	`Router(config)#`
		Specifies the address of one or more Domain Name System (DNS) servers to use for name and address resolution.

Step 3	**ip dhcp excluded-address** *low-address* [*high-address*] **Example:** `Router(config)# ip dhcp excluded-address 192.168.9.0`	Specifies IP addresses that the DHCP server should not assign to DHCP clients. This example excludes the router address.

Step 4	**ip dhcp pool** *name*
	Example:
	`Router(config)# ip dhcp pool dpool1`
	`Router(config-dhcp)#`
		Creates a DHCP address pool on the router and enters DHCP pool configuration mode.
		• The *name* argument can be a string or an integer.

Step 5	**network** *network-number* [*mask* | *prefix-length*]
	Example:
	`Router(config-dhcp)# network 10.10.0.0 255.255.255.0`
	`Router(config-dhcp)#`
		Defines the subnet number (IP) address for the DHCP address pool, optionally including the mask.

Step 6	**import all**
	Example:
	`Router(config-dhcp)# import all`
	`Router(config-dhcp)#`
		Imports DHCP option parameters into the DHCP portion of the router database.

Step 7	**default-router** *address* [*address2...address8*]
	Example:
	`Router(config-dhcp)# default-router 10.10.10.10`
	`Router(config-dhcp)#`
		Specifies up to eight default routers for a DHCP client.

Step 8	**dns-server** *address* [*address2...address8*]
	Example:
	`Router(config-dhcp)# dns-server 192.168.35.2`
	`Router(config-dhcp)#`
		Specifies up to 8 DNS servers available to a DHCP client.

	Command or Action	Purpose

Step 9	**domain-name** *domain*
	Example:
	`Router(config-dhcp)# domain-name cisco.com`
	`Router(config-dhcp)#`
		Specifies the domain name for a DHCP client.

Step 10	**exit**
	Example:
	`Router(config-dhcp)# exit`
	`Router(config)#`
		Exits DHCP configuration mode, and enters global configuration mode.

Configuration Example

The following configuration example shows a portion of the configuration file for the DCHP configuration described in this chapter.

```
ip dhcp excluded-address 192.168.9.0
!
ip dhcp pool dpool1
   import all
   network 10.10.0.0 255.255.255.0
   default-router 10.10.10.10
   dns-server 192.168.35.2
   domain-name cisco.com
!
ip domain name smallbiz.com
ip name-server 192.168.11.12
```

Verify Your DHCP Configuration

Use the following commands to view your DHCP configuration.

- **show ip dhcp import**—Displays the optional parameters imported into the DHCP server database.
- **show ip dhcp pool**—Displays information about the DHCP address pools.
- **show ip dhcp server statistics**—Displays the DHCP server statistics, such as the number of address pools and bindings.

```
Router# show ip dhcp import
Address Pool Name: dpool1

Router# show ip dhcp pool
Pool dpool1 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 10.10.0.1            10.10.0.1        - 10.10.0.254       0

Router# show ip dhcp server statistics
```

```
Memory usage         15419
Address pools        1
Database agents      0
Automatic bindings   0
Manual bindings      0
Expired bindings     0
Malformed messages   0
Secure arp entries   0

Message              Received
BOOTREQUEST          0
DHCPDISCOVER         0
DHCPREQUEST          0
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

Message              Sent
BOOTREPLY            0
DHCPOFFER            0
DHCPACK              0
DHCPNAK              0
Router#
```

Configure VLANs

To configure VLANs on your router, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **vlan** *vlan_id*
2. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**vlan** *vlan_id* **Example:** `Router(config)# vlan 2`	Adds VLANs, with identifiers ranging from 1-4094.
Step 2	**exit** **Example:** `Router(config)# exit`	Updates the VLAN database, propagates it throughout the administrative domain, and returns to privileged EXEC mode.

Assign a Switch Port to a VLAN

To assign a switch port to a VLAN, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **interface** *switch port id*
2. **switchport access vlan** *vlan-id*
3. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**interface** *switch port id*
	Example:
	`Router(config)# interface FastEthernet 2`
	`Router(config-if)#`
		Specifies the switch port that you assign to the VLAN.

Step 2	**switchport access vlan** *vlan-id*
	Example:
	`Router(config-if)# switchport access vlan 2`
	`Router(config-if)#`
		Assigns a port to the VLAN.

Step 3	**end**
	Example:
	`Router(config-if)# end`
	`Router#`
		Exits interface mode and returns to privileged EXEC mode.

Verify Your VLAN Configuration

Use the following commands to view your VLAN configuration.

- **show**—Entered from VLAN database mode. Displays summary configuration information for all configured VLANs.
- **show vlan-switch**—Entered from privileged EXEC mode. Displays detailed configuration information for all configured VLANs.

```
Router# vlan database
Router(vlan)# show

  VLAN ISL Id: 1
    Name: default
    Media Type: Ethernet
    VLAN 802.10 Id: 100001
    State: Operational
    MTU: 1500
    Translational Bridged VLAN: 1002
    Translational Bridged VLAN: 1003

  VLAN ISL Id: 2
    Name: VLAN0002
    Media Type: Ethernet
    VLAN 802.10 Id: 100002
    State: Operational
    MTU: 1500

  VLAN ISL Id: 3
    Name: red-vlan
    Media Type: Ethernet
    VLAN 802.10 Id: 100003
    State: Operational
    MTU: 1500

  VLAN ISL Id: 1002
    Name: fddi-default
    Media Type: FDDI
    VLAN 802.10 Id: 101002
    State: Operational
    MTU: 1500
    Bridge Type: SRB
    Translational Bridged VLAN: 1
    Translational Bridged VLAN: 1003

  VLAN ISL Id: 1003
    Name: token-ring-default
    Media Type: Token Ring
    VLAN 802.10 Id: 101003
    State: Operational
    MTU: 1500
    Bridge Type: SRB
    Ring Number: 0
    Bridge Number: 1
    Parent VLAN: 1005
    Maximum ARE Hop Count: 7
    Maximum STE Hop Count: 7
    Backup CRF Mode: Disabled
    Translational Bridged VLAN: 1
    Translational Bridged VLAN: 1002

  VLAN ISL Id: 1004
    Name: fddinet-default
    Media Type: FDDI Net
    VLAN 802.10 Id: 101004
    State: Operational
    MTU: 1500
    Bridge Type: SRB
    Bridge Number: 1
    STP Type: IBM

  VLAN ISL Id: 1005
    Name: trnet-default
    Media Type: Token Ring Net
    VLAN 802.10 Id: 101005
    State: Operational
    MTU: 1500
    Bridge Type: SRB
    Bridge Number: 1
    STP Type: IBM

Router# show vlan-switch

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0, Fa1, Fa3
2    VLAN0002                         active    Fa2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
2    enet  100002     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        1      1003
1003 tr    101003     1500  1005   0      -        -    srb      1      1002
1004 fdnet 101004     1500  -      -      1        ibm  -        0      0
1005 trnet 101005     1500  -      -      1        ibm  -        0      0
```

CHAPTER 15

Configuring a VPN Using Easy VPN and an IPSec Tunnel

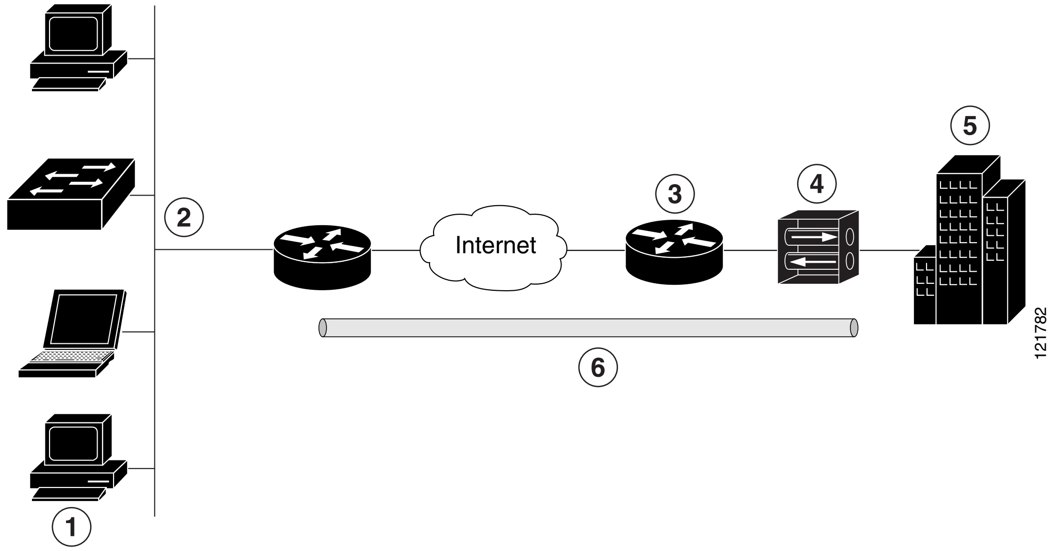
This chapter provides an overview of the creation of Virtual Private Networks (VPNs) that can be configured on the Cisco 860 and Cisco 880 series Integrated Services Routers (ISRs).

Cisco routers and other broadband devices provide high-performance connections to the Internet, but many applications also require the security of VPN connections, which perform a high level of authentication and which encrypt the data between two particular endpoints.

Two types of VPNs are supported—site-to-site and remote access. Site-to-site VPNs are used to connect branch offices to corporate offices, for example. Remote access VPNs are used by remote clients to log in to a corporate network.

The example in this chapter illustrates the configuration of a remote access VPN that uses the Cisco Easy VPN and an IP Security (IPSec) tunnel to configure and secure the connection between the remote client and the corporate network. Figure 15-1 shows a typical deployment scenario.

Figure 15-1 Remote Access VPN Using IPSec Tunnel



1	Remote, networked users
2	VPN client—Cisco 860 and Cisco 880 series ISRs
3	Router—Providing the corporate office network access
4	VPN server—Easy VPN server
5	Corporate office with a network address of 10.1.1.1
6	IPSec tunnel

Cisco Easy VPN

The Cisco Easy VPN client feature eliminates much of the tedious configuration work by implementing the Cisco Unity Client protocol. This protocol allows most VPN parameters, such as internal IP addresses, internal subnet masks, DHCP server addresses, WINS server addresses, and split-tunneling flags, to be defined at a VPN server that is acting as an IPSec server.

An Easy VPN server-enabled device can terminate VPN tunnels initiated by mobile and remote workers who are running Cisco Easy VPN Remote software on PCs. Easy VPN server-enabled devices allow remote routers to act as Easy VPN Remote nodes.

The Cisco Easy VPN client feature can be configured in one of two modes—client mode or network extension mode. Client mode is the default configuration and allows only devices at the client site to access resources at the central site. Resources at the client site are unavailable to the central site. Network extension mode allows users at the central site to access network resources on the client site.

After the IPSec server has been configured, a VPN connection can be created with minimal configuration on an IPSec client, such as a supported Cisco 860 and Cisco 880 series ISRs. When the IPSec client initiates the VPN tunnel connection, the IPSec server pushes the IPSec policies to the IPSec client and creates the corresponding VPN tunnel connection.

Note The Cisco Easy VPN client feature supports configuration of only one destination peer. If your application requires creation of multiple VPN tunnels, you must manually configure the IPSec VPN and Network Address Translation/Peer Address Translation (NAT/PAT) parameters on both the client and the server.

Configuration Tasks

Perform the following tasks to configure your router for this network scenario:

- Configure the IKE Policy
- Configure Group Policy Information
- Apply Mode Configuration to the Crypto Map
- Enable Policy Lookup
- Configure IPSec Transforms and Protocols
- Configure the IPSec Crypto Method and Parameters
- Apply the Crypto Map to the Physical Interface
- Create an Easy VPN Remote Configuration

An example showing the results of these configuration tasks is provided in the "Configuration Example" section on page 15-12.

Note The procedures in this chapter assume that you have already configured basic router features as well as PPPoE or PPPoA with NAT, DCHP and VLANs. If you have not performed these configurations tasks, see Chapter 3, "Basic Router Configuration," Chapter 13, "Configuring PPP over Ethernet with NAT," Chapter 14, "Configuring PPP over ATM with NAT," and Chapter 13, "Configuring a LAN with DHCP and VLANs" as appropriate for your router.

Note The examples shown in this chapter refer only to the endpoint configuration on the Cisco 870 series router. Any VPN connection requires both endpoints to be configured properly to function. See the software configuration documentation as needed to configure the VPN for other router models.

Configure the IKE Policy

To configure the Internet Key Exchange (IKE) policy, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **crypto isakmp policy** *priority*
2. **encryption** {**des** | **3des** | **aes** | **aes 192** | **aes 256**}
3. **hash** {**md5** | **sha**}
4. **authentication** {**rsa-sig** | **rsa-encr** | **pre-share**}

5. **group** {**1** | **2** | **5**}
6. **lifetime** *seconds*
7. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**crypto isakmp policy** *priority*
	Example:
	`Router(config)# crypto isakmp policy 1`
	`Router(config-isakmp)#`
		Creates an IKE policy that is used during IKE negotiation. The priority is a number from 1 to 10000, with 1 being the highest.
		Also enters the Internet Security Association Key and Management Protocol (ISAKMP) policy configuration mode.

Step 2	**encryption** {**des** | **3des** | **aes** | **aes 192** | **aes 256**}
	Example:
	`Router(config-isakmp)# encryption 3des`
	`Router(config-isakmp)#`
		Specifies the encryption algorithm used in the IKE policy.
		The example specifies 168-bit data encryption standard (DES).

Step 3	**hash** {**md5** | **sha**}
	Example:
	`Router(config-isakmp)# hash md5`
	`Router(config-isakmp)#`
		Specifies the hash algorithm used in the IKE policy.
		The example specifies the Message Digest 5 (MD5) algorithm. The default is Secure Hash standard (SHA-1).

Step 4	**authentication** {**rsa-sig** | **rsa-encr** | **pre-share**}
	Example:
	`Router(config-isakmp)# authentication pre-share`
	`Router(config-isakmp)#`
		Specifies the authentication method used in the IKE policy.
		The example specifies a pre-shared key.

Step 5	**group** {**1** | **2** | **5**}
	Example:
	`Router(config-isakmp)# group 2`
	`Router(config-isakmp)#`
		Specifies the Diffie-Hellman group to be used in an IKE policy.

Step 6	**lifetime** *seconds*
	Example:
	`Router(config-isakmp)# lifetime 480`
	`Router(config-isakmp)#`
		Specifies the lifetime, in seconds, for an IKE security association (SA).
		• Acceptable values are from 60 to 86400.

Step 7	**exit**
	Example:
	`Router(config-isakmp)# exit`
	`Router(config)#`
		Exits ISAKMP policy configuration mode and returns to global configuration mode.

Configure Group Policy Information

To configure the group policy, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **crypto isakmp client configuration group** {**group-name** | **default**}
2. **key** *name*
3. **dns** *primary-server*
4. **domain** *name*
5. **exit**
6. **ip local pool** {**default** | *poolname*} [*low-ip-address* [*high-ip-address*]]

DETAILED STEPS

	Command or Action	Purpose

Step 1	**crypto isakmp client configuration group** {**group-name** | **default**}
	Example:
	`Router(config)# crypto isakmp client configuration group rtr-remote`
	`Router(config-isakmp-group)#`
		Creates an IKE policy group containing attributes to be downloaded to the remote client.
		Also enters the Internet Security Association Key and Management Protocol (ISAKMP) group policy configuration mode.

Step 2	**key** *name*
	Example:
	`Router(config-isakmp-group)# key secret-password`
	`Router(config-isakmp-group)#`
		Specifies the IKE pre-shared key for the group policy.

Step 3	**dns** *primary-server*
	Example:
	`Router(config-isakmp-group)# dns 10.50.10.1`
	`Router(config-isakmp-group)#`
		Specifies the primary Domain Name System (DNS) server for the group.
		Note To specify Windows Internet Naming Service (WINS) servers for the group, use the **wins** command.

Step 4	**domain** *name*
	Example:
	`Router(config-isakmp-group)# domain company.com`
	`Router(config-isakmp-group)#`
		Specifies group domain membership.

	Command or Action	Purpose

Step 5	**exit**
	Example:
	`Router(config-isakmp-group)# exit`
	`Router(config)#`
		Exits ISAKMP policy configuration mode and returns to global configuration mode.

Step 6	**ip local pool** {**default** | *poolname*} [*low-ip-address* [*high-ip-address*]]
	Example:
	`Router(config)# ip local pool dynpool 30.30.30.20 30.30.30.30`
	`Router(config)#`
		Specifies a local address pool for the group.
		For details about this command and additional parameters that can be set, see *Cisco IOS Dial Technologies Command Reference*.

Apply Mode Configuration to the Crypto Map

To apply mode configuration to the crypto map, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **crypto map** *map-name* **isakmp authorization list** *list-name*
2. **crypto map** *tag* **client configuration address** [**initiate** | **respond**]

DETAILED STEPS

	Command or Action	Purpose

Step 1	**crypto map** *map-name* **isakmp authorization list** *list-name*
	Example:
	`Router(config)# crypto map dynmap isakmp authorization list rtr-remote`
	`Router(config)#`
		Applies mode configuration to the crypto map and enables key lookup (IKE queries) for the group policy from an authentication, authorization, and accounting (AAA) server.

Step 2	**crypto map** *tag* **client configuration address** [**initiate** | **respond**]
	Example:
	`Router(config)# crypto map dynmap client configuration address respond`
	`Router(config)#`
		Configures the router to reply to mode configuration requests from remote clients.

Enable Policy Lookup

To enable policy lookup through AAA, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **aaa new-model**
2. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
3. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2...*]
4. **username** *name* {**nopassword** | **password** *password* | **password** *encryption-type encrypted-password*}

DETAILED STEPS

	Command or Action	Purpose

Step 1	**aaa new-model**
	Example:
	`Router(config)# aaa new-model`
	`Router(config)#`
		Enables the AAA access control model.

Step 2	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
	Example:
	`Router(config)# aaa authentication login rtr-remote local`
	`Router(config)#`
		Specifies AAA authentication of selected users at login, and specifies the method used.
		• This example uses a local authentication database.
		Note You could also use a RADIUS server for this. For details, see *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference*.

Step 3	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2...*]]
	Example:
	`Router(config)# aaa authorization network rtr-remote local`
	`Router(config)#`
		Specifies AAA authorization of all network-related service requests, including PPP, and specifies the method of authorization.
		• This example uses a local authorization database.
		Note You could also use a RADIUS server for this. For details, see the *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference*.

Step 4	**username** *name* {**nopassword** | **password** *password* | **password** *encryption-type encrypted-password*}
	Example:
	`Router(config)# username Cisco password 0 Cisco`
	`Router(config)#`
		Establishes a username-based authentication system.

Configure IPSec Transforms and Protocols

A transform set represents a certain combination of security protocols and algorithms. During IKE negotiation, the peers agree to use a particular transform set for protecting data flow.

During IKE negotiations, the peers search in multiple transform sets for a transform that is the same at both peers. When such a transform set is found, it is selected and applied to the protected traffic as a part of both peer configurations.

To specify the IPSec transform set and protocols, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]
2. **crypto ipsec security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}

DETAILED STEPS

	Command or Action	Purpose

Step 1	**crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]
	Example:
	`Router(config)# crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac`
	`Router(config)#`
		Defines a transform set—an acceptable combination of IPSec security protocols and algorithms.
		See *Cisco IOS Security Command Reference* for details about the valid transforms and combinations.

Step 2	**crypto ipsec security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}
	Example:
	`Router(config)# crypto ipsec security-association lifetime seconds 86400`
	`Router(config)#`
		Specifies global lifetime values used when IPSec security associations are negotiated.
		See *Cisco IOS Security Command Reference* for details.

Note With manually established security associations, there is no negotiation with the peer, and both sides must specify the same transform set.

Configure the IPSec Crypto Method and Parameters

A dynamic crypto map policy processes negotiation requests for new security associations from remote IPSec peers, even if the router does not know all the crypto map parameters (for example, IP address).

To configure the IPSec crypto method, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **crypto dynamic-map** *dynamic-map-name dynamic-seq-num*
2. **set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*]
3. **reverse-route**
4. **exit**
5. **crypto map** *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*]

DETAILED STEPS

	Command or Action	Purpose

Step 1	**crypto dynamic-map** *dynamic-map-name dynamic-seq-num*
	Example:
	`Router(config)# crypto dynamic-map dynmap 1`
	`Router(config-crypto-map)#`
		Creates a dynamic crypto map entry and enters crypto map configuration mode.
		See *Cisco IOS Security Command Reference* for details about this command.

Step 2	**set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*]
	Example:
	`Router(config-crypto-map)# set transform-set vpn1`
	`Router(config-crypto-map)#`
		Specifies which transform sets can be used with the crypto map entry.

Step 3	**reverse-route**
	Example:
	`Router(config-crypto-map)# reverse-route`
	`Router(config-crypto-map)#`
		Creates source proxy information for the crypto map entry.
		See *Cisco IOS Security Command Reference* for details.

Step 4	**exit**
	Example:
	`Router(config-crypto-map)# exit`
	`Router(config)#`
		Exits crypto map configuration mode and returns to global configuration mode.

Step 5	**crypto map** *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*]
	Example:
	`Router(config)# crypto map static-map 1 ipsec-isakmp dynamic dynmap`
	`Router(config)#`
		Creates a crypto map profile.

Apply the Crypto Map to the Physical Interface

The crypto maps must be applied to each interface through which IP Security (IPSec) traffic flows. Applying the crypto map to the physical interface instructs the router to evaluate all the traffic against the security associations database. With the default configurations, the router provides secure connectivity by encrypting the traffic sent between remote sites. However, the public interface still allows the rest of the traffic to pass and provides connectivity to the Internet.

To apply a crypto map to an interface, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **interface** *type number*
2. **crypto map** *map-name*
3. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**interface** *type number*
	Example:
	`Router(config)# interface fastethernet 4`
	`Router(config-if)#`
		Enters the interface configuration mode for the interface to which the crypto map applies.

Step 2	**crypto map** *map-name*
	Example:
	`Router(config-if)# crypto map static-map`
	`Router(config-if)#`
		Applies the crypto map to the interface.
		See *Cisco IOS Security Command Reference* for details about this command.

Step 3	**exit**
	Example:
	`Router(config-crypto-map)# exit`
	`Router(config)#`
		Exits interface configuration mode and returns to global configuration mode.

Create an Easy VPN Remote Configuration

The router acting as the IPSec remote router must create an Easy VPN remote configuration and assign it to the outgoing interface.

To create the remote configuration, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **crypto ipsec client ezvpn** *name*
2. **igroup** *group-name* **key** *group-key*
3. **peer** {*ipaddress* | *hostname*}
4. **mode** {**client** | **network-extension** | **network extension plus**}

5. **exit**
6. **interface** *type number*
7. **crypto ipsec client ezvpn** *name* [**outside** | **inside**]
8. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**crypto ipsec client ezvpn** *name*
	Example:
	`Router(config)# crypto ipsec client ezvpn ezvpnclient`
	`Router(config-crypto-ezvpn)#`
		Creates a Cisco Easy VPN remote configuration, and enters Cisco Easy VPN remote configuration mode.

Step 2	**group** *group-name* **key** *group-key*
	Example:
	`Router(config-crypto-ezvpn)# group ezvpnclient key secret-password`
	`Router(config-crypto-ezvpn)#`
		Specifies the IPSec group and IPSec key value for the VPN connection.

Step 3	**peer** {*ipaddress* | *hostname*}
	Example:
	`Router(config-crypto-ezvpn)# peer 192.168.100.1`
	`Router(config-crypto-ezvpn)#`
		Specifies the peer IP address or hostname for the VPN connection.
		Note A hostname can be specified only when the router has a DNS server available for hostname resolution.

Step 4	**mode** {**client** | **network-extension** | **network extension plus**}
	Example:
	`Router(config-crypto-ezvpn)# mode client`
	`Router(config-crypto-ezvpn)#`
		Specifies the VPN mode of operation.

Step 5	**exit**
	Example:
	`Router(config-crypto-ezvpn)# exit`
	`Router(config)#`
		Exits Cisco Easy VPN remote configuration mode and returns to global configuration mode.

Step 6	**interface** *type number*
	Example:
	`Router(config)# interface fastethernet 4`
	`Router(config-if)#`
		Enters the interface configuration mode for the interface to which the Cisco Easy VPN remote configuration applies.
		Note For routers with an ATM WAN interface, this command would be **interface atm 0**.

	Command or Action	Purpose

Step 7	**crypto ipsec client ezvpn** *name* [**outside** | **inside**]
	Example:
	`Router(config-if)# crypto ipsec client ezvpn ezvpnclient outside`
	`Router(config-if)#`
		Assigns the Cisco Easy VPN remote configuration to the WAN interface.
		This command causes the router to automatically create the NAT or port address translation (PAT) and access list configuration needed for the VPN connection.

Step 8	**exit**
	Example:
	`Router(config-crypto-ezvpn)# exit`
	`Router(config)#`
		Exits interface configuration mode and returns to global configuration mode.

Verifying Your Easy VPN Configuration

```
Router# show crypto ipsec client ezvpn

Tunnel name :ezvpnclient
Inside interface list:vlan 1
Outside interface:fastethernet 4
Current State:IPSEC_ACTIVE
Last Event:SOCKET_UP
Address:8.0.0.5
Mask:255.255.255.255
Default Domain:cisco.com
```

Configuration Example

The following configuration example shows a portion of the configuration file for the VPN and IPSec tunnel described in this chapter.

```
!
aaa new-model
!
aaa authentication login rtr-remote local
aaa authorization network rtr-remote local
aaa session-id common
!
username Cisco password 0 Cisco
!
crypto isakmp policy 1
    encryption 3des
    authentication pre-share
    group 2
    lifetime 480
!
crypto isakmp client configuration group rtr-remote
    key secret-password
    dns 10.50.10.1 10.60.10.1
    domain company.com
    pool dynpool
!
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
```

```
!
crypto ipsec security-association lifetime seconds 86400
!
crypto dynamic-map dynmap 1
    set transform-set vpn1
    reverse-route
!
crypto map static-map 1 ipsec-isakmp dynamic dynmap
crypto map dynmap isakmp authorization list rtr-remote
crypto map dynmap client configuration address respond

crypto ipsec client ezvpn ezvpnclient
    connect auto
    group 2 key secret-password
    mode client
    peer 192.168.100.1
!

interface fastethernet 4
    crypto ipsec client ezvpn ezvpnclient outside
    crypto map static-map
!
interface vlan 1
    crypto ipsec client ezvpn ezvpnclient inside
!
```

CHAPTER 16

Configuring Cisco Multimode G.SHDSL EFM/ATM

This chapter provides a link to a document that describes the configuration of the Cisco Multimode 4-pair G.SHDSL Ethernet in the first mile (EFM)/Asynchronous Transfer Mode (ATM) WAN port. This functionality is provided by the Cisco C888-EA-K9 fixed Integrated Services Router (ISR).

The following guide describes this functionality for multiple products, including enhanced high-speed WAN interface cards (EHWICs) and the C888-EA-K9 router:

Configuring Cisco Multimode G.SHDSL EFM/ATM in Cisco ISR G2, available at the following location:

http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/GSHDSL_EFM_ATM_HWICS.html

CHAPTER 17

Deployment Scenarios

In the following sections, this chapter describes and shows some typical deployment scenarios for the Cisco 860, Cisco 880, and Cisco 890 series Intergrated Services Routers (ISRs):

About the Deployment Scenarios

This chapter describes typical deployment scenarios for Cisco ISRs, and provides a high-level overview of each scenario with pointers to information about new functions.

Major features of the Cisco ISRs include:

- 3G wireless data connectivity backup (some Cisco 880 series ISRs)
- Voice capabilities (some Cisco 880 series ISRs)
- Embedded wireless device (optional)
- Power over Ethernet (all Cisco 880 series ISRs)

3G Wireless Backup

Some Cisco 880 series ISRs have 3G wireless data backup capability. See Chapter 6, "Configuring Backup Data Lines and Remote Management" for details.

Voice

Some Cisco 880 series ISRs contain voice capabilities. Refer to the *Cisco IOS Voice Configuration Library* for details.

Embedded Wireless Device

- Cisco 860 series, Cisco 880 series, and Cisco 890 ISRs have an optional wireless device that runs its own version of the Cisco IOS software.
  - Cisco 890 Series ISRs with embedded access points are eligible to upgrade from autonomous software to Cisco Unified software, if the router is running the IP Base feature set and Cisco IOS 12.4(22)YB software.
  - 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 12.4(20)T software.
  - Cisco 860 Series ISRs with embedded access points are not eligible to upgrade from autonomous software to Cisco Unified software.

Note To use the embedded access point in a Cisco Unified Architecture, the Cisco Wireless LAN Configuration (WLC) must be running version 5.1 or later.

See Chapter 9, “Basic Wireless Device Configuration” for upgrade information.

Power Over Ethernet

All Cisco 880 Series ISRs contain PoE capabilities. See *Cisco 860 Series, Cisco 880 Series, and Cisco 890 Series Integrated Services Routers Hardware Installation Guide* for details.

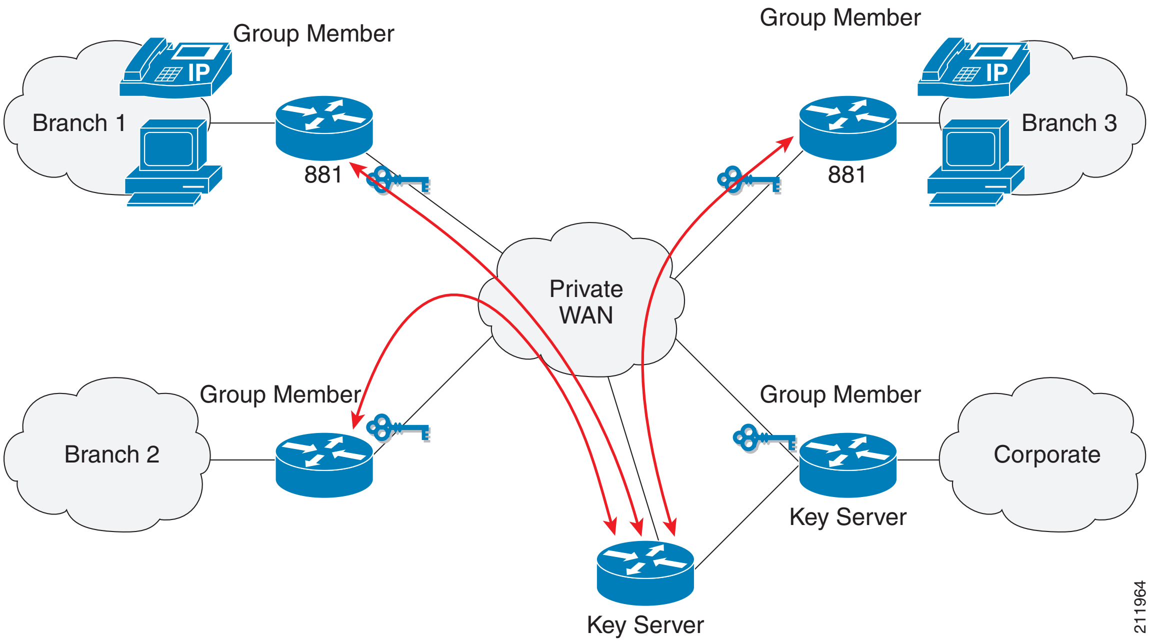
Enterprise Small Branch

Figure 17-1 shows an Enterprise Small Branch deployment that uses the following technologies and features:

- Group Encrypted Transport VPN (GETVPN) for highly scalable secure branch connectivity
- Cisco IOS firewall (FW) policies that secure the front line of network connectivity and provide network and application layer protection to the enterprise network

- Voice and multicast applications
- Quality of service (QoS) prioritizes critical applications and ensures timely delivery of latency-sensitive and mission-critical applications

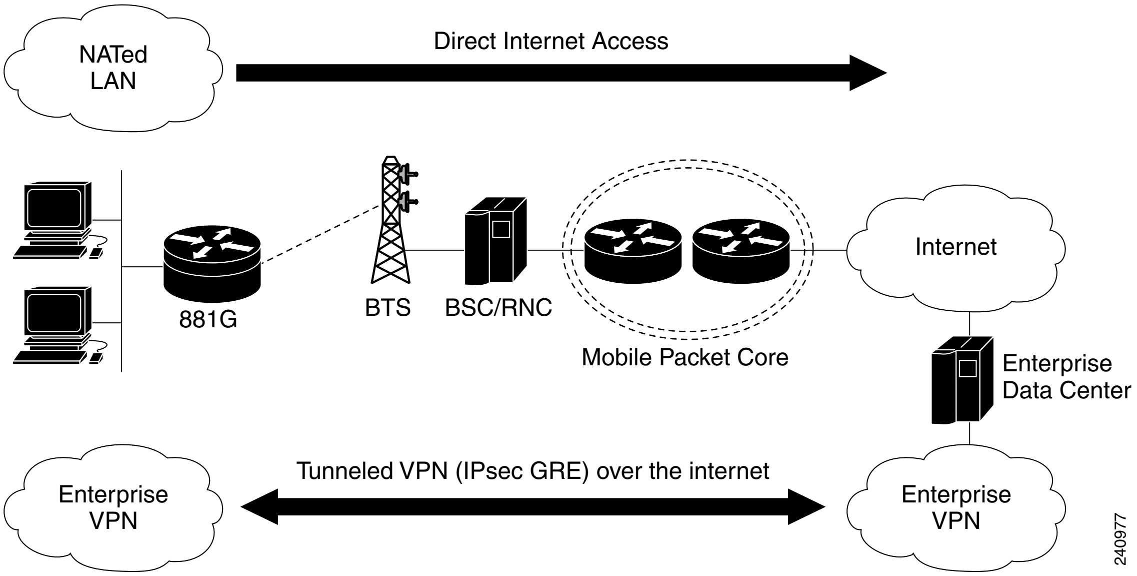
Figure 17-1 Enterprise Small Branch



Internet Service and IPSec VPN with 3G

Figure 17-2 shows a remote office deployment that uses 3G wireless technology for both backup and primary applications to communicate to their enterprise data center. Besides providing direct Internet access employing Network Address Translation (NAT), Cisco 880 series ISRs can provide tunneled Virtual Private Network (VPN) service using IP Security and Generic Routing Encapsulation (IPSec+GRE) for secure and private communication over the public Internet.

Figure 17-2 Internet Service and IPSec VPN with 3G



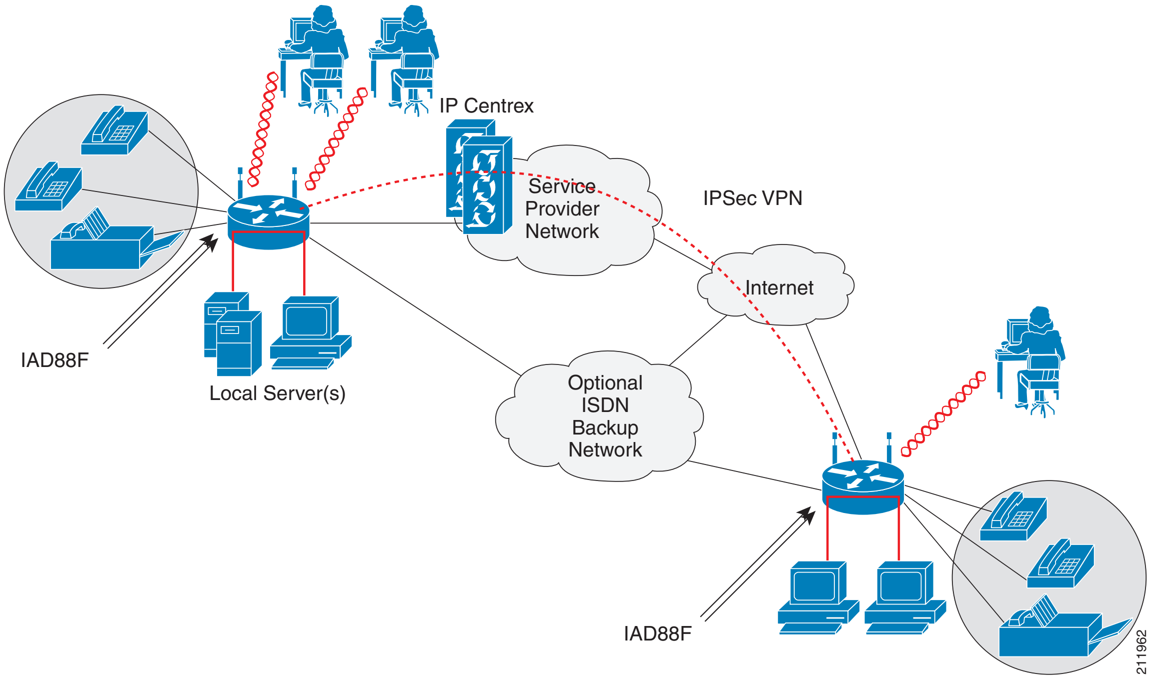
SMB Applications

Figure 17-3 shows a small-to medium-size business deployment (SMB) that uses the following technologies and features at each branch office:

- Easy VPN with Virtual Tunnel Interface (VTI) to simplify secure VPN for remote offices and teleworkers.
- Deep packet inspection firewall for security. Firewalls provide the first level of access checking. They work with other security technologies, including intrusion prevention, encryption, and endpoint security, to provide a well-rounded defense-in-depth enterprise security system.
- Inline Intrusion Prevention Systems (IPS) protection provides additional security, and is a core facet of the Cisco Self-Defending Network. Cisco IOS IPS helps enable the network to defend itself with the intelligence to accurately classify, identify, and stop or block malicious or damaging traffic in real time.
- QoS provides timely delivery of latency-sensitive and mission-critical applications.

- ISDN connectivity backup provides network redundancy in the event that the primary service provider link fails.
- Support for existing analog voice and fax capabilities.

Figure 17-3 Small-to Medium-Size Business



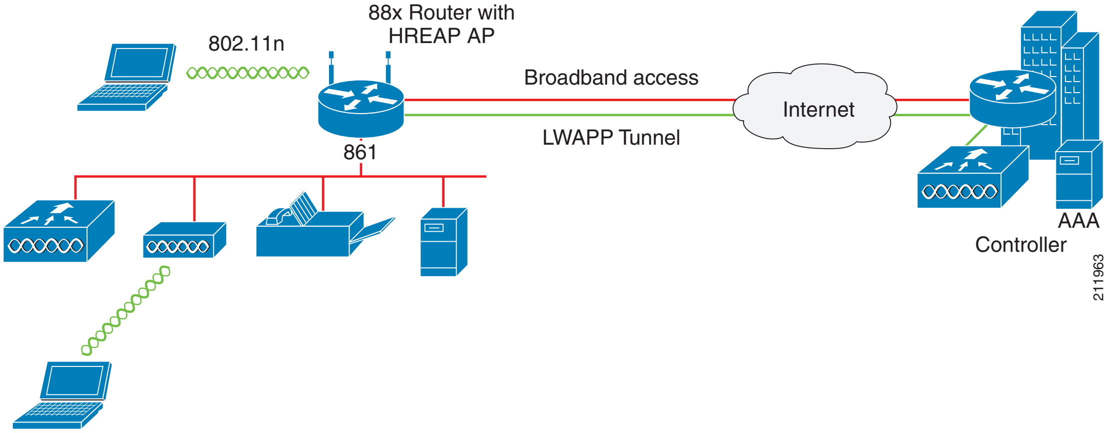
Enterprise Wireless Deployments with LWAPP

Figure 17-4 shows an Enterprise wireless LAN deployment using Lightweight Access Point Protocol (LWAPP) and the following technologies and features:

- Broadband Internet access and VPN connection to a central site.
- Hybrid Remote Edge Access Point (H-REAP) provides wireless LAN services to remote and branch offices without using a wireless LAN controller at each location. With HREAP, organizations can bridge traffic locally, tunnel traffic over the WAN, or tunnel traffic over LWAPP on a per Service Set Identifier (SSID).

- Dynamic RF management with Cisco Wireless Control System (WCS).
- Ability to mix and match embedded access points with external access points.

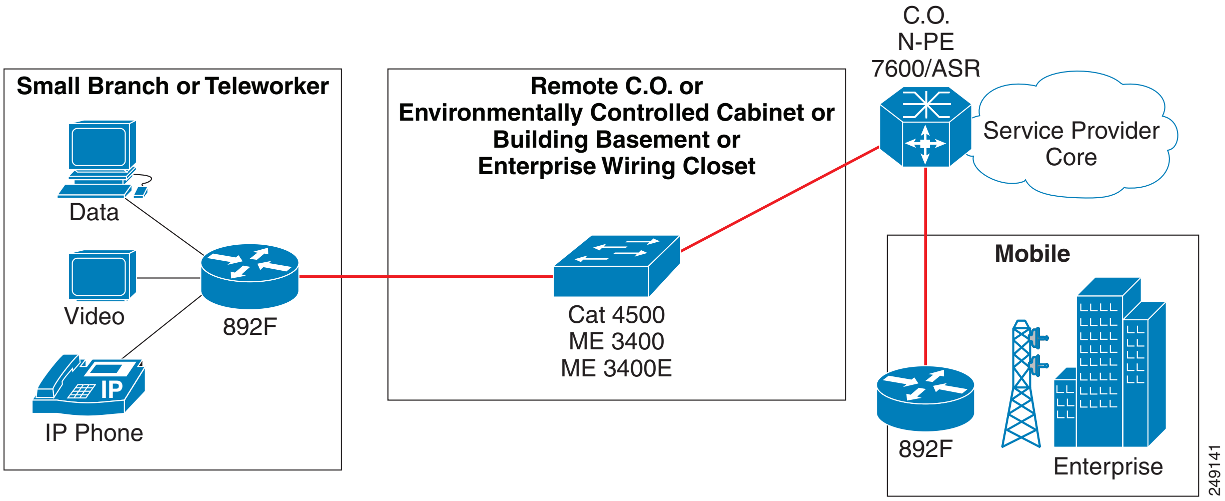
Figure 17-4 Wireless LAN with LWAPP



Enterprise Small Branch Office Deployment

Figure 17-5 shows a small branch office or teleworker deployment that uses a gigabit Ethernet fiber connection through the SFP port.

Figure 17-5 Enterprise Small Branch office Deployment



CHAPTER 18

Troubleshooting

Use the information in this chapter to help isolate problems you might encounter or to rule out the router as the source of a problem. This chapter contains the following sections:

Getting Started

Before troubleshooting a software problem, you must connect a terminal or PC to the router by using the light-blue console port. (For information on making this connection, see the documentation listed in the "Related Documentation" section on page xviii.) With a connected terminal or PC, you can view status messages from the router and enter commands to troubleshoot a problem.

You can also remotely access the interface (Ethernet, ADSL, or telephone) by using Telnet. The Telnet option assumes that the interface is up and running.

Before Contacting Cisco or Your Reseller

If you cannot locate the source of a problem, contact your local reseller for advice. Before you call, you should have the following information ready:

- Chassis type and serial number
- Maintenance agreement or warranty information
- Type of software and version number

- Date you received the hardware
- Brief description of the problem
- Brief description of the steps you have taken to isolate the problem

ADSL Troubleshooting

If you experience trouble with the ADSL connection, verify the following:

- The ADSL line is connected and is using pins 3 and 4. For more information on the ADSL connection, see the hardware guide for your router.
- The ADSL CD LED is on. If it is not on, the router may not be connected to the DSL access multiplexer (DSLAM). For more information on the ADSL LEDs, see the hardware installation guide specific for your router.
- The correct Asynchronous Transfer Mode (ATM) virtual path identifier/virtual circuit identifier (VPI/VCI) is being used.
- The DSLAM supports discrete multi-tone (DMT) Issue 2.
- The ADSL cable that you connect to the Cisco router must be 10BASE-T Category 5, unshielded twisted-pair (UTP) cable. Using regular telephone cable can introduce line errors.

SHDSL Troubleshooting

Symmetrical high-data-rate digital subscriber line (SHDSL) is available on the Cisco 888 routers. If you experience trouble with the SHDSL connection, verify the following:

- The SHDSL line is connected and using pins 3 and 4. For more information on the G.SHDSL connection, see the hardware guide for your router.
- The G.SHDSL LED is on. If it is not on, the router may not be connected to the DSL access multiplexer (DSLAM). For more information on the G.SHDSL LED, see the hardware installation guide specific for your router.
- The correct asynchronous transfer mode (ATM) virtual path identifier/virtual circuit identifier (VPI/VCI) is being used.
- The DSLAM supports the G.SHDSL signaling protocol.

Use the **show controllers dsl 0** command in EXEC mode to view an SHDSL configuration.

VDSL2 Troubleshooting

Very-high-data-rate digital subscriber line 2 (VDSL2) is available on the Cisco 887 routers. If you experience trouble with the VDSL2 connection, verify the following:

- The VDSL2 line is connected and using pins 3 and 4. For more information on the VDSL2 connection, see the hardware guide for your router.
- The VDSL2 LED CD light is on. If it is not on, the router may not be connected to the DSL access multiplexer (DSLAM). For more information on the VDSL2 LED, see the hardware installation guide specific for your router.
- The DSLAM supports the VDSL2 signaling protocol.

Use the **show controllers vdsl 0** command in EXEC mode to view a VDSL2 configuration. The **debug vdsl 0 daemon state** command can be used to enable the debug messages that print the state transition of VDSL2 training.

If there is trouble with the VDSL firmware file, you can reload or upgrade it without upgrading your Cisco IOS image. Use the command:

controller vdsl 0 firmware *flash:<firmware file name>*

to load the firmware file into the VDSL modem chipset. Then enter **shutdown/no shutdown** commands on the controller vdsl 0 interface. After this, the new firmware will be downloaded and the VDSL2 line starts training up.

Note Cisco 860VAE series ISRs require that the router be reloaded (IOS reload) before the new VDSL firmware will be loaded.

If the command is not present or the named firmware file is corrupt or not available, the default firmware file *flash:vdsl.bin* is checked to be present and not corrupt. The firmware in this file is then downloaded to the modem chipset.

Note Cisco 860VAE series ISRs will state the reason of failure during bootup if the new VDSL firmware fails to load after IOS reload.

show interfaces Troubleshooting Command

Use the **show interface**s command to display the status of all physical ports (Ethernet, Fast Ethernet, and ATM) and logical interfaces on the router. Table 18-1 describes messages in the command output.

Example 18-1 Viewing Status of Ethernet or Fast Ethernet Interfaces

```
Router# show interfaces ethernet 0 **similar output for show interfaces fastethernet 0
command **
Ethernet0 is up, line protocol is up
Hardware is PQUICC Ethernet, address is 0000.0c13.a4db
(bia0010.9181.1281)
Internet address is 170.1.4.101/24
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255., txload 1/255, rxload 1/255
    Encapsulation ARPA, loopback not set
    Keepalive set (10 sec)
```

Example 18-2 Viewing Status of ATM Interfaces

```
Router# show interfaces atm 0
ATM0 is up, line protocol is up
  Hardware is PQUICC_SAR (with Alcatel ADSL Module)
  Internet address is 14.0.0.16/8
  MTU 1500 bytes, sub MTU 1500, BW 640 Kbit, DLY 80 usec,
     reliability 40/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Keepalive not supported
  Encapsulation(s):AAL5, PVC mode
  10 maximum active VCs, 1 current VCCs
  VC idle disconnect time:300 seconds
  Last input 01:16:31, output 01:16:31, output hang never
  Last clearing of "show interface" counters never
  Input queue:0/75/0 (size/max/drops); Total output drops:0
  Queueing strategy:Per VC Queueing
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     512 packets input, 59780 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 1024 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     426 packets output, 46282 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Example 18-3 Viewing Status of Dialer Interfaces

```
Router# show interfaces dialer 1
Dialer 1 is up, line protocol is up
    Hardware is Dialer interface
    Internet address is 1.1.1.1/24
    MTU 1500 bytes, BW 100000 Kbit, DLY 100000 usec, reliability
        255/255. txload 1/255, rxload 1/255
    Encapsulation PPP, loopback not set
    Keepalive set (10 sec)
DTR is pulsed for 5 seconds on reset
LCP Closed
```

Table 18-1 describes possible command output for the **show interfaces** command.

Table 18-1 show interfaces Command Output Description

Output	Cause
For ATM Interfaces	
ATM 0 is up, line protocol is up	The ATM line is up and operating correctly.
ATM 0 is down, line protocol is down	• The ATM interface has been disabled with the **shutdown** command. or • The ATM line is down, possibly because the ADSL cable is disconnected or because the wrong type of cable is connected to the ATM port.
ATM 0.*n* is up, line protocol is up	The specified ATM subinterface is up and operating correctly.
ATM 0.*n* is administratively down, line protocol is down	The specified ATM subinterface has been disabled with the **shutdown** command.
ATM 0.*n* is down, line protocol is down	The specified ATM subinterface is down, possibly because the ATM line has been disconnected (by the service provider).
For Ethernet/Fast Ethernet Interfaces	
Ethernet/Fast Ethernet *n* is up, line protocol is up	The specified Ethernet/Fast Ethernet interface is connected to the network and operating correctly.

Table 18-1 show interfaces Command Output Description (continued)

Output	Cause
Ethernet/Fast Ethernet *n* is up, line protocol is down	The specified Ethernet/Fast Ethernet interface has been correctly configured and enabled, but the Ethernet cable might be disconnected from the LAN.
Ethernet/Fast Ethernet *n* is administratively down, line protocol is down	The specified Ethernet/Fast Ethernet interface has been disabled with the **shutdown** command, and the interface is disconnected.
For Dialer Interfaces	
Dialer *n* is up, line protocol is up	The specified dialer interface is up and operating correctly.
Dialer *n* is down, line protocol is down	• This is a standard message and may not indicate anything is actually wrong with the configuration. or • If you are having problems with the specified dialer interface, this can mean it is not operating, possibly because the interface has been brought down with the **shutdown** command, or the ADSL cable is disconnected.

Troubleshooting—Debug Commands

The following tables list the debug commands specific to each feature. The Cisco IOS Master Command List at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html provides more information on the usage guidelines for these commands.

Note Before you run any debug command listed in the following tables, ensure that you run the **logging buffered debugging** command and turn off console debug using the **no logging console debugging** command.

Table 18-2 Troubleshooting—Debug Commands

Debug Command	Purpose
Configuring NID on L3 Interface	
debug ethernet nid configuration	Enables debugging of configuration-related issues.
debug ethernet nid packet egress	Enables debugging of packet-processing (vlan tag push) related issues on egress side.
debug ethernet nid packet ingress	Enables debugging of packet-processing (vlan tag pop) related issues on ingress side.
Configuring Ethernet Data Plane Loopback	
debug elb-pal-pd-error configuration	Awaiting inputs from Engineering
debug elb-pal-pd-event configuration	Awaiting inputs from Engineering

Table 18-2 Troubleshooting—Debug Commands (continued)

Debug Command	Purpose
debug elb-pal-pd-all configuration	Awaiting inputs from Engineering
Configuring CFM on Routed Port and Port MEP	
debug ethernet cfm all	Enables all Ethernet CFM debug messages.
debug ethernet cfm diagnostic	Enables low-level diagnostic debugging of Ethernet CFM general events or packet-related events.
debug ethernet cfm error	Enables debugging of Ethernet CFM errors.
debug ethernet cfm packets	Enables debugging of Ethernet CFM message packets.
debug ecfmpal all	Enables debug messages for all Ethernet CFM platform events.
debug ecfmpal api	Displays debug messages for all Ethernet CFM platform API events.
debug ecfmpal common	Displays debug messages for all Ethernet CFM platform common events.
debug ecfmpal ecfmpal	Enables debugging of all Ethernet CFM platform events.
debug ecfmpal epl	Enables debugging of all Ethernet CFM platform endpoint-list (EPL) events.
debug ecfmpal isr	Enables debugging of all Ethernet CFM platform interrupt service request (ISR) events.
Configuring Y.1731 on Routed Port	
debug epmpal all	Enables debugging of all Ethernet performance monitoring (PM) events.
debug epmpal api	Enables debugging of Ethernet PM API events.
debug epmpal rx	Enables debugging of Ethernet PM packet-receive events.
debug epmpal tx	Enables debugging of Ethernet PM packet-transmit events.

ATM Troubleshooting Commands

Use the following commands to troubleshoot your ATM interface.

- ping atm interface Command
- show atm interface Command
- debug atm Commands

ping atm interface Command

Use the **ping atm interface** command to determine whether a particular PVC is in use. The PVC does not need to be configured on the router to use this command. Example 18-4 shows the use of this command to determine whether PVC 8/35 is in use.

Example 18-4 Determining If a PVC Is in Use

```
Router# ping atm interface atm 0 8 35 seg-loopback

Type escape sequence to abort.
Sending 5, 53-byte segment OAM echoes, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 148/148/148 ms
```

This command sends five OAM F5 loopback packets to the DSLAM (segment OAM packets). If the PVC is configured at the DSLAM, the ping is successful.

To test whether the PVC is being used at the aggregator, enter the following command:

```
Router# ping atm interface atm 0 8 35 end-loopback

Type escape sequence to abort.
Sending 5, 53-byte end-to-end OAM echoes, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 400/401/404 ms
```

This command sends end-to-end OAM F5 packets, which are echoed back by the aggregator.

show atm interface Command

To display ATM-specific information about an ATM interface, use the **show atm interface atm 0** command from privileged EXEC mode, as shown in Example 18-5.

Example 18-5 Viewing Information About an ATM Interface

```
Router# show atm interface atm 0
Interface ATM0:
AAL enabled: AAL5 , Maximum VCs:11, Current VCCs:0

Maximum Transmit Channels:0
Max. Datagram Size:1528
PLIM Type:INVALID - 640Kbps, Framing is INVALID,
DS3 lbo:short, TX clocking:LINE
0 input, 0 output, 0 IN fast, 0 OUT fast
Avail bw = 640
Config. is ACTIVE
```

Table 18-3 describes some of the fields shown in the command output.

Table 18-3 show atm interface Command Output Description

Field	Description
ATM interface	Interface number. Always 0 for the Cisco 860 and Cisco 880 series access routers.
AAL enabled	Type of AAL enabled. The Cisco 860 and Cisco 880 series access routers support AAL5.

Table 18-3 show atm interface Command Output Description (continued)

Field	Description
Maximum VCs	Maximum number of virtual connections this interface supports.
Current VCCs	Number of active virtual channel connections (VCCs).
Maximum Transmit Channels	Maximum number of transmit channels.
Max Datagram Size	Configured maximum number of bytes in the largest datagram.
PLIM Type	Physical layer interface module (PLIM) type.

debug atm Commands

Use the **debug** commands to troubleshoot configuration problems that you might be having on your network. The **debug** commands provide extensive, informative displays to help you interpret any possible problems.

Guidelines for Using Debug Commands

Read the following guidelines before using debug commands to ensure appropriate results.

- All debug commands are entered in privileged EXEC mode.
- To view debugging messages on a console, enter the **logging console debug** command.
- Most **debug** commands take no arguments.
- To disable debugging, enter the **undebug all** command.
- To use **debug** commands during a Telnet session on your router, enter the **terminal monitor** command.

Caution Debugging is assigned a high priority in your router CPU process, and it can render your router unusable. For this reason, use **debug** commands only to troubleshoot specific problems. The best time to use debug commands is during periods of low network traffic so that other activity on the network is not adversely affected.

You can find additional information and documentation about the **debug** commands in the *Cisco IOS Debug Command Reference*.

debug atm errors Command

Use the **debug atm errors** command to display ATM errors. The **no** form of this command disables debugging output. Example 18-6 shows a sample output.

Example 18-6 Viewing ATM Errors

```
Router# debug atm errors
ATM errors debugging is on
Router#
01:32:02:ATM(ATM0.2):VC(3) Bad SAP received 4500
01:32:04:ATM(ATM0.2):VC(3) Bad SAP received 4500
01:32:06:ATM(ATM0.2):VC(3) Bad SAP received 4500
01:32:08:ATM(ATM0.2):VC(3) Bad SAP received 4500
01:32:10:ATM(ATM0.2):VC(3) Bad SAP received 4500
```

debug atm events Command

Use the **debug atm events** command to display events that occur on the ATM interface processor and to diagnose problems in an ATM network. This command provides an overall picture of the stability of the network. The **no** form of this command disables debugging output.

If the interface is successfully communicating with the Digital Subscriber Line Access Multiplexer (DSLAM) at the telephone company, the modem state is 0x10. If the interface is not communicating with the DSLAM, the modem state is 0x8. Example 18-7 shows an ADSL line that is up and training successfully. Example 18-8 shows an ADSL line that is not communicating correctly. Note that the modem state does not transition to 0x10.

Example 18-7 Viewing ATM Interface Processor Events—Success

```
Router# debug atm events
Router#
00:02:57: DSL: Send ADSL_OPEN command.
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Sent command 0x5
00:02:57: DSL: Received response: 0x26
00:02:57: DSL: Unexpected response 0x26
00:02:57: DSL: Send ADSL_OPEN command.
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Sent command 0x5
00:03:00: DSL: 1: Modem state = 0x8
00:03:02: DSL: 2: Modem state = 0x10
00:03:05: DSL: 3: Modem state = 0x10
00:03:07: DSL: 4: Modem state = 0x10
00:03:09: DSL: Received response: 0x24
00:03:09: DSL: Showtime!
00:03:09: DSL: Sent command 0x11
00:03:09: DSL: Received response: 0x61
00:03:09: DSL: Read firmware revision 0x1A04
00:03:09: DSL: Sent command 0x31
00:03:09: DSL: Received response: 0x12
00:03:09: DSL: operation mode 0x0001
00:03:09: DSL: SM: [DMTDSL_DO_OPEN -> DMTDSL_SHOWTIME]
```

Example 18-8 Viewing ATM Interface Processor Events—Failure

```
Router# debug atm events
Router#
00:02:57: DSL: Send ADSL_OPEN command.
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Sent command 0x5
00:02:57: DSL: Received response: 0x26
00:02:57: DSL: Unexpected response 0x26
00:02:57: DSL: Send ADSL_OPEN command.
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Sent command 0x5
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
```

debug atm packet Command

Use the **debug atm packet** command to display all process-level ATM packets for both outbound and inbound packets. The output reports information online when a packet is received or a transmission is attempted. The **no** form of this command disables debugging output.

Caution Because the **debug atm packet** command generates a significant amount of output for every packet processed, use it only when network traffic is low, so that other system activities are not adversely affected.

The command syntax is:

debug atm packet [**interface atm** *number* [**vcd** *vcd-number*][**vc** *vpi/vci number*]]

no debug atm packet [**interface atm** *number* [**vcd** *vcd-number*][**vc** *vpi/vci number*]]

where the keywords are defined as follows:

interface atm *number*	(Optional) ATM interface or subinterface number.
vcd *vcd-number*	(Optional) Number of the virtual circuit designator (VCD).
vc *vpi/vci number*	VPI/VCI value of the ATM PVC.

Example 18-9 shows sample output for the **debug atm packet** command.

Example 18-9 Viewing ATM Packet Processing

```
Router# debug atm packet
Router#
01:23:48:ATM0(O):
VCD:0x1 VPI:0x1 VCI:0x64 DM:0x0 SAP:AAAA CTL:03 OUI:000000 TYPE:0800 Length:0x70
01:23:48:4500 0064 0008 0000 FF01 9F80 0E00 0010 0E00 0001 0800 A103 0AF3 17F7 0000
01:23:48:0000 004C BA10 ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD
01:23:48:ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD
01:23:48:ABCD ABCD ABCD ABCD ABCD
01:23:48:
01:23:48:ATM0(I):
VCD:0x1 VPI:0x1 VCI:0x64 Type:0x0 SAP:AAAA CTL:03 OUI:000000 TYPE:0800 Length:0x70
01:23:48:4500 0064 0008 0000 FE01 A080 0E00 0001 0E00 0010 0000 A903 0AF3 17F7 0000
01:23:48:0000 004C BA10 ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD
01:23:48:ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD
01:23:48:ABCD ABCD ABCD ABCD ABCD
01:23:48:
```

Table 18-4 describes some of the fields shown in the **debug atm packet** command output.

Table 18-4 debug atm packet Command Output Description

Field	Description
ATM0	Interface that is generating the packet.
(O)	Output packet. (I) would mean receive packet.
VCD: 0x*n*	Virtual circuit associated with this packet, where *n* is some value.
VPI: 0x*n*	Virtual path identifier for this packet, where *n* is some value.

Table 18-4 debug atm packet Command Output Description (continued)

Field	Description
DM: 0x*n*	Descriptor mode bits, where *n* is some value.
Length: *n*	Total length of the packet (in bytes) including the ATM headers.

Software Upgrade Methods

Several methods are available for upgrading software on the Cisco 860 and Cisco 880 series Integrated Services Routers, including:

- Copy the new software image to flash memory over the LAN or WAN while the existing Cisco IOS software image is operating.
- Copy the new software image to flash memory over the LAN while the boot image (ROM monitor) is operating.
- Copy the new software image over the console port while in ROM monitor mode.
- From ROM monitor mode, boot the router from a software image that is loaded on a TFTP server. To use this method, the TFTP server must be on the same LAN as the router.

Recovering a Lost Password

To recover a lost enable or lost enable-secret password:

1. Change the Configuration Register
2. Reset the Router
3. Reset the Password and Save Your Changes (for lost enable secret passwords only)
4. Reset the Configuration Register Value

Note Recovering a lost password is only possible when you are connected to the router through the console port. These procedures cannot be performed through a Telnet session.

Tip See the “Hot Tips” section on Cisco.com for additional information on replacing enable secret passwords.

Change the Configuration Register

To change a configuration register, follow these steps:

Step 1 Connect an ASCII terminal or a PC running a terminal emulation program to the CONSOLE port on the Fthe router.

Step 2 Configure the terminal to operate at 9600 baud, 8 data bits, no parity, and 1 stop bit.

Step 3 At the privileged EXEC prompt (*router_name* #), enter the **show version** command to display the existing configuration register value (shown in bold at the bottom of this output example):

```
Router# show version
Cisco IOS Software, C880 Software (C880-ADVENTERPRISEK9-M), Version 12.3(nightly
.PCBU_WIRELESS041110) NIGHTLY BUILD, synced to haw_t_pi1_pcbu HAW_T_PI1_PCBU_200
40924
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Thu 11-Nov-04 03:37 by jsomebody

ROM: System Bootstrap, Version 1.0.0.6(20030916:100755) [jsomebody],
 DEVELOPMENT SOFTWARE

Router uptime is 2467 minutes
System returned to ROM by power-on
System image file is "flash:c880-adventerprisek9-mz.pcbu_wireless.041110"

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
use. Delivery of Cisco cryptographic products does not imply
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco 877 (MPC8272) processor (revision 0x00) with 59392K/6144K bytes of memory.

Processor board ID
MPC8272 CPU Rev: Part Number 0xC, Mask Number 0x10
4 FastEthernet interfaces
1 ATM interface
1 802.11 Radio
128K bytes of non-volatile configuration memory.
20480K bytes of processor board System flash (Intel Strataflash)

Configuration register is 0x2102
```

Step 4 Record the setting of the configuration register.

Step 5 To enable the break setting (indicated by the value of bit 8 in the configuration register), enter the **config-register 0x01** command from privileged EXEC mode.

- Break enabled—Bit 8 is set to 0.
- Break disabled (default setting)—Bit 8 is set to 1.

Reset the Router

To reset the router, follow these steps:

Step 1 If break is enabled, go to Step 2. If break is disabled, turn the router off (O), wait 5 seconds, and turn it on (|) again. Within 60 seconds, press the **Break** key. The terminal displays the ROM monitor prompt. Go to Step 3.

Note Some terminal keyboards have a key labeled *Break*. If your keyboard does not have a Break key, see the documentation that came with the terminal for instructions on how to send a break.

Step 2 Press **break**. The terminal displays the following prompt:

```
rommon 2>
```

Step 3 Enter **confreg 0x142** to reset the configuration register:

```
rommon 2> confreg 0x142
```

Step 4 Initialize the router by entering the **reset** command:

```
rommon 2> reset
```

The router cycles its power, and the configuration register is set to 0x142. The router uses the boot ROM system image, indicated by the system configuration dialog:

```
--- System Configuration Dialog ---
```

Step 5 Enter **no** in response to the prompts until the following message is displayed:

```
Press RETURN to get started!
```

Step 6 Press **Return**. The following prompt appears:

```
Router>
```

Step 7 Enter the **enable** command to enter enable mode. Configuration changes can be made only in enable mode:

```
Router> enable
```

The prompt changes to the privileged EXEC prompt:

```
Router#
```

Step 8 Enter the **show startup-config** command to display an enable password in the configuration file:

```
Router# show startup-config
```

If you are recovering an enable password, do not perform the steps in the following "Reset the Password and Save Your Changes" section. Instead, complete the password recovery process by performing the steps in the "Reset the Configuration Register Value" section.

If you are recovering an enable secret password, it is not displayed in the **show startup-config** command output. Complete the password recovery process by performing the steps in the following "Reset the Password and Save Your Changes" section.

Reset the Password and Save Your Changes

To reset your password and save the changes, follow these steps:

Step 1 Enter the **configure terminal** command to enter global configuration mode:

```
Router# configure terminal
```

Step 2 Enter the **enable secret** command to reset the enable secret password in the router:

```
Router(config)# enable secret password
```

Step 3 Enter **exit** to exit global configuration mode:

```
Router(config)# exit
```

Step 4 Save your configuration changes:

```
Router# copy running-config startup-config
```

Reset the Configuration Register Value

To reset the configuration register value after you have recovered or reconfigured a password, follow these steps:

Step 1 Enter the **configure terminal** command to enter global configuration mode:

```
Router# configure terminal
```

Step 2 Enter the **configure register** command and the original configuration register value that you recorded.

```
Router(config)# config-reg value
```

Step 3 Enter **exit** to exit configuration mode:

```
Router(config)# exit
```

Note To return to the configuration being used before you recovered the lost enable password, do not save the configuration changes before rebooting the router.

Step 4 Reboot the router, and enter the recovered password.

Cisco Configuration Professional Express

After you connect the cables and power up the router, we recommend that you use the Cisco CP Express web-based application to configure the initial router settings.

For instructions on how to use Cisco CP Express to configure the router see the *Cisco CP Express User's Guide*.

Cisco IOS Software Basic Skills

Understanding how to use Cisco IOS software can save you time when you are configuring your router. This appendix contains the following sections which provide basic information:

- Configuring the Router from a PC, page A-1
- Understanding Command Modes, page A-2
- Getting Help, page A-4
- Enable Secret Passwords and Enable Passwords, page A-5
- Entering Global Configuration Mode, page A-5
- Using Commands, page A-6
- Saving Configuration Changes, page A-7
- Summary, page A-7
- Where to Go Next, page A-7

If you are already familiar with Cisco IOS software, go to one of the following chapters:

- Chapter 3, "Basic Router Configuration"
- Chapter 17, "Deployment Scenarios"

Configuring the Router from a PC

You can configure your router from a PC that is connected through the console port by using terminal emulation software. The PC uses this software to send commands to your router. Table A-1 lists some common types of terminal emulation software that you can use, depending on the operating system that you are running.

Table A-1 Types of Terminal Emulation Software

PC Operating System	Terminal Emulation Software
Windows 95, Windows 98, Windows 2000, Windows NT, Windows XP	HyperTerm (included with Windows software), ProComm Plus
Windows 3.1	Terminal (included with Windows software)
Macintosh	ProComm, VersaTerm

You can use the terminal emulation software to change settings for the router that is connected to the PC. Configure the software to the following standard VT-100 emulation settings so that your PC can communicate with your router:

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

These settings should match the default settings of your router. To change the router baud, data bits, parity, or stop bits settings, you must reconfigure parameters in the ROM monitor. For more information, see Appendix C, "ROM Monitor." To change the router flow control setting, use the **flowcontrol** command in global configuration mode.

For information on how to enter global configuration mode so that you can configure your router, see the "Entering Global Configuration Mode" section later in this chapter.

Understanding Command Modes

This section describes the Cisco IOS command mode structure. Each command mode supports specific Cisco IOS commands. For example, you can use the **interface** *type number* command only from global configuration mode.

The following Cisco IOS command modes are hierarchical. When you begin a router session, you are in user EXEC mode.

- User EXEC
- Privileged EXEC
- Global configuration

Table A-2 lists the command modes that are used in this guide, describes how to access each mode, shows the prompt for each mode, and explains how to exit to a mode or enter another mode. Because each mode configures different router elements, you might need to enter and exit modes frequently. You can see a list of available commands for a particular mode by entering a question mark (?) at the prompt. For a description of each command, including syntax, see the Cisco IOS Release 12.3 documentation set.

Table A-2 Command Modes Summary

Mode	Access Method	Prompt	Mode Exit and Entrance	About This Mode
User EXEC	Begin a session with your router.	`Router>`	To exit a router session, enter the **logout** command.	Use this mode to: • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	Enter the **enable** command from user EXEC mode.	`Router#`	• To exit to user EXEC mode, enter the **disable** command. • To enter global configuration mode, enter the **configure** command.	Use this mode to: • Configure your router operating parameters. • Perform the verification steps shown in this guide. To prevent unauthorized changes to your router configuration, protect access to this mode by using a password as described in the "Enable Secret Passwords and Enable Passwords" procedure on page A-5.
Global configuration	Enter the **configure** command from privileged EXEC mode.	`Router (config)#`	• To exit to privileged EXEC mode, enter the **exit** or **end** command, or press **Ctrl-Z**. • To enter interface configuration mode, enter the **interface** command.	Use this mode to configure parameters that apply to your router globally. From this mode you can access the following modes: • Interface configuration • Router configuration • Line configuration
Interface configuration	Enter the **interface** command (with a specific interface, such as **interface atm 0**) from global configuration mode.	`Router (config-if)#`	• To exit to global configuration mode, enter the **exit** command. • To exit to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**. • To enter subinterface configuration mode, specify a subinterface by using the **interface** command.	Use this mode to configure parameters for the router Ethernet and serial interfaces or subinterfaces.

Table A-2 Command Modes Summary (continued)

Mode	Access Method	Prompt	Mode Exit and Entrance	About This Mode
Router configuration	Enter one of the **router** commands followed by the appropriate keyword—for example **router rip**—from global configuration mode.	`Router (config-router)#`	• To exit to global configuration mode, enter the **exit** command. • To exit to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.	Use this mode to configure an IP routing protocol.
Line configuration	Enter the **line** command with the desired line number and optional line type, for example, **line 0**, from global configuration mode.	`Router (config-line)#`	• To exit to global configuration mode, enter the **exit** command. • To exit to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.	Use this mode to configure parameters for the terminal line.

Getting Help

You can use the question mark (?) and arrow keys to help you enter commands.

For a list of available commands for a prticular command mode, enter a question mark:

```
Router> ?
access-enable  Create a temporary access-list entry
access-profile Apply user-profile to interface
clear          Reset functions
.
.
.
```

To complete a command, enter a few known characters followed by a question mark (with no space):

```
Router> sh?
* s=show set show slip systat
```

For a list of command variables, enter the command followed by a space and a question mark:

```
Router> show ?
.
.
.
clock       Display the system clock
dialer      Dialer parameters and statistics
exception   exception information
.
.
.
```

To redisplay a command that you previously entered, press the **Up Arrow** key. You can continue to press the **Up Arrow** key for more commands.

Enable Secret Passwords and Enable Passwords

By default, the router ships without password protection. Because many privileged EXEC commands are used to set operating parameters, you should password-protect these commands to prevent unauthorized use.

You can use two commands to do this:

- **enable secret** *password*—A very secure, encrypted password.
- **enable** *password*—A less secure, unencrypted local password.

Both the **enable** and **enable secret** passwords control access to various privilege levels (0 to 15). The **enable** password is intended for local use and is thus unencrypted. The **enable secret** password is intended for network use; that is, in environments where the password crosses the network or is stored on a TFTP server. You must enter an **enable secret** or **enable** password with a privilege level of 1 to gain access to privileged EXEC mode commands.

For maximum security, the passwords should be different. If you enter the same password for both during the setup process, your router accepts the passwords, but warns you that they should be different.

An **enable secret** password can contain from 1 to 25 uppercase and lowercase alphanumeric characters. An **enable** password can contain any number of uppercase and lowercase alphanumeric characters. In both cases, a number cannot be the first character. Spaces are also valid password characters; for example, *two words* is a valid password. Leading spaces are ignored; trailing spaces are recognized.

Entering Global Configuration Mode

To make any configuration changes to your router, you must be in global configuration mode. This section describes how to enter global configuration mode while using a terminal or PC that is connected to your router console port.

To enter global configuration mode, follow these steps:

Step 1 After your router boots up, enter the **enable** or **enable secret** command:

```
Router> enable
```

Step 2 If you have configured your router with an enable password, enter it when you are prompted.

The enable password does not appear on the screen when you enter it. This example shows how to enter privileged EXEC mode:

```
Password: enable_password
Router#
```

Privileged EXEC mode is indicated by the pound sign (#) in the prompt. You can now make changes to your router configuration.

Step 3 Enter the **configure terminal** command to enter global configuration mode:

```
Router# configure terminal
Router(config)#
```

You can now make changes to your router configuration.

Using Commands

This section provides some tips about entering Cisco IOS commands at the command-line interface (CLI).

Abbreviating Commands

You only have to enter enough characters for the router to recognize the command as unique. This example shows how to enter the **show version** command:

```
Router # sh v
```

Undoing Commands

If you want to disable a feature or undo a command that you entered, you can enter the keyword **no** before most commands; for example, **no ip routing**.

Command-Line Error Messages

Table A-3 lists some error messages that you might encounter while using the CLI to configure your router.

Table A-3 Common CLI Error Messages

Error Message	Meaning	How to Get Help
`% Ambiguous command: "show con"`	You did not enter enough characters for your router to recognize the command.	Reenter the command, followed by a question mark (**?**) with no space between the command and the question mark. The possible keywords that you can enter with the command are displayed.
`% Incomplete command.`	You did not enter all the keywords or values required by this command.	Reenter the command, followed by a question mark (**?**) with no space between the command and the question mark. The possible keywords that you can enter with the command are displayed.
`% Invalid input detected at '^' marker.`	You entered the command incorrectly. The error occurred where the caret mark (^) appears.	Enter a question mark (**?**) to display all the commands that are available in this particular command mode.

Saving Configuration Changes

You must enter the **copy running-config startup-config** command to save your configuration changes toNVRAM so that they are not lost if there is a system reload or power outage. This example shows how to use this command to save your changes:

```
Router# copy running-config startup-config
Destination filename [startup-config]?
```

Press **Return** to accept the default destination filename *startup-config*, or enter your desired destination filename and press **Return**.

It might take a minute or two to save the configuration to NVRAM. After the configuration has been saved, the following message appears:

```
Building configuration...
Router#
```

Summary

Now that you have reviewed some Cisco IOS software basics, you can begin to configure your router. Remember:

- You can use the question mark (**?**) and arrow keys to help you enter commands.
- Each command mode restricts you to a set of commands. If you are having difficulty entering a command, check the prompt, and then enter the question mark (**?**) for a list of available commands. You might be in the wrong command mode or using the wrong syntax.
- To disable a feature, enter the keyword **no** before the command; for example, **no ip routing**.
- Save your configuration changes to NVRAM so that they are not lost if there is a system reload or power outage.

Where to Go Next

To configure your router, go to Chapter 3, “Basic Router Configuration,” and Chapter 17, “Deployment Scenarios.”

APPENDIX B

Concepts

This appendix contains conceptual information that may be useful to Internet service providers or network administrators when they configure Cisco routers. To review some typical network scenarios, see Chapter 17, "Deployment Scenarios."

The following topics are included in this appendix:

ADSL

ADSL is a technology that allows both data and voice to be transmitted over the same line. It is a packet-based network technology that allows high-speed transmission over twisted-pair copper wire on the local loop ("last mile") between a network service provider (NSP) central office and the customer site, or on local loops created within either a building or a campus.

The benefit of ADSL over a serial or dialup line is that it is always on and always connected, increasing bandwidth and lowering the costs compared with a dialup or leased line. ADSL technology is asymmetric in that it allows more bandwidth from an NSP central office to the customer site than from the customer site to the central office. This asymmetry, combined with always-on access (which eliminates call setup), makes ADSL ideal for Internet and intranet surfing, video on demand, and remote LAN access.

SHDSL

SHDSL is a technology based on the G.SHDSL (G.991.2) standard that allows both data and voice to be transmitted over the same line. SHDSL is a packet-based network technology that allows high-speed transmission over twisted-pair copper wire between a network service provider (NSP) central office and a customer site, or on local loops created within either a building or a campus.

G.SHDSL devices can extend the reach from central offices and remote terminals to approximately 26,000 feet (7925 m), at symmetrical data rates from 72 kbps up to 2.3 Mbps. In addition, it is repeatable at lower speeds, which means there is virtually no limit to its reach.

SHDSL technology is symmetric in that it allows equal bandwidth between an NSP central office and a customer site. This symmetry, combined with always-on access (which eliminates call setup), makes SHDSL ideal for LAN access.

Network Protocols

Network protocols enable the network to pass data from its source to a specific destination over LAN or WAN links. Routing address tables are included in the network protocols to provide the best path for moving the data through the network.

IP

The best-known Transmission Control Protocol/Internet Protocol (TCP/IP) at the internetwork layer is IP, which provides the basic packet delivery service for all TCP/IP networks. In addition to the physical node addresses, the IP protocol implements a system of logical host addresses called IP addresses. The IP addresses are used by the internetwork and higher layers to identify devices and to perform internetwork routing. The Address Resolution Protocol (ARP) enables IP to identify the physical address that matches a given IP address.

IP is used by all protocols in the layers above and below it to deliver data, which means that all TCP/IP data flows through IP when it is sent and received regardless of its final destination.

IP is a connectionless protocol, which means that IP does not exchange control information (called a *handshake*) to establish an end-to-end connection before transmitting data. In contrast, a connection-oriented protocol exchanges control information with the remote computer to verify that it is ready to receive data before sending it. When the handshaking is successful, the computers have established a connection. IP relies on protocols in other layers to establish the connection if connection-oriented services are required.

Internet Packet Exchange (IPX) exchanges routing information using Routing Information Protocol (RIP), a dynamic distance-vector routing protocol. RIP is described in more detail in the following sections.

Routing Protocol Options

Routing protocols include the following:

- Routing Information Protocol (RIP)
- Enhanced Interior Gateway Routing Protocol (Enhanced IGRP)

RIP and Enhanced IGRP differ in several ways, as shows Table B-1.

Table B-1 RIP and Enhanced IGRP Comparison

Protocol	Ideal Topology	Metric	Routing Updates
RIP	Suited for topologies with 15 or fewer hops.	Hop count. Maximum hop count is 15. Best route is one with lowest hop count.	By default, every 30 seconds. You can reconfigure this value and also use triggered extensions to RIP.
Enhanced IGRP	Suited for large topologies with 16 or more hops to reach a destination.	Distance information. Based on a successor, which is a neighboring router that has a least-cost path to a destination that is guaranteed to not be part of a routing loop.	Hello packets sent every 5 seconds, as well as incremental updates sent when the state of a destination changes.

RIP

RIP is an associated protocol for IP, and is widely used for routing protocol traffic over the Internet. RIP is a distance-vector routing protocol, which means that it uses distance (hop count) as its metric for route selection. *Hop count* is the number of routers that a packet must traverse to reach its destination. For example, if a particular route has a hop count of 2, then a packet must traverse two routers to reach its destination.

By default, RIP routing updates are broadcast every 30 seconds. You can reconfigure the interval at which the routing updates are broadcast. You can also configure triggered extensions to RIP so that routing updates are sent only when the routing database is updated. For more information on triggered extensions to RIP, see the Cisco IOS Release 12.3 documentation set.

Enhanced IGRP

Enhanced IGRP is an advanced Cisco-proprietary distance-vector and link-state routing protocol, which means it uses a metric more sophisticated than distance (hop count) for route selection. Enhanced IGRP uses a metric based on a successor, which is a neighboring router that has a least-cost path to a destination that is guaranteed not to be part of a routing loop. If a successor for a particular destination does not exist but neighbors advertise the destination, the router must recompute a route.

Each router that is running Enhanced IGRP sends hello packets every 5 seconds to inform neighboring routers that it is functioning. If a particular router does not send a hello packet within a prescribed period, Enhanced IGRP assumes that the state of a destination has changed and sends an incremental update.

Because Enhanced IGRP supports IP, you can use one routing protocol for multiprotocol network environments, minimizing the size of the routing tables and the amount of routing information.

PPP Authentication Protocols

The Point-to-Point Protocol (PPP) encapsulates network-layer protocol information over point-to-point links.

PPP originated as an encapsulation protocol for transporting IP traffic over point-to-point links. PPP also established a standard for the assignment and management of IP addresses, asynchronous (start/stop) and bit-oriented synchronous encapsulation, network protocol multiplexing, link configuration, link quality testing, error detection, and option negotiation for such capabilities as network-layer address negotiation and data-compression negotiation. PPP supports these functions by providing an extensible Link Control Protocol (LCP) and a family of Network Control Protocols (NCPs) to negotiate optional configuration parameters and facilities.

The current implementation of PPP supports two security authentication protocols to authenticate a PPP session:

- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)

PPP with PAP or CHAP authentication is often used to inform the central site which remote routers are connected to it.

PAP

PAP uses a two-way handshake to verify the passwords between routers. To understand how PAP works, imagine a network topology in which a remote office Cisco router is connected to a corporate office Cisco router. After the PPP link is established, the remote office router repeatedly sends a configured username and password until the corporate office router accepts the authentication.

PAP has the following characteristics:

- The password portion of the authentication is sent across the link in clear text (not scrambled or encrypted).
- PAP provides no protection from playback or repeated trial-and-error attacks.
- The remote office router controls the frequency and timing of the authentication attempts.

CHAP

CHAP uses a three-way handshake to verify passwords. To understand how CHAP works, imagine a network topology in which a remote office Cisco router is connected to a corporate office Cisco router.

After the PPP link is established, the corporate office router sends a challenge message to the remote office router. The remote office router responds with a variable value. The corporate office router checks the response against its own calculation of the value. If the values match, the corporate office router accepts the authentication. The authentication process can be repeated anytime after the link is established.

CHAP has the following characteristics:

- The authentication process uses a variable challenge value rather than a password.
- CHAP protects against playback attack through the use of the variable challenge value, which is unique and unpredictable. Repeated challenges limit the time of exposure to any single attack.
- The corporate office router controls the frequency and timing of the authentication attempts.

Note We recommend using CHAP because it is the more secure of the two protocols.

TACACS+

Cisco 860 and Cisco 880 series routers support the Terminal Access Controller Access Control System Plus (TACACS+) protocol through Telnet. TACACS+ is a Cisco-proprietary authentication protocol that provides remote access authentication and related network security services, such as event logging. User passwords are administered in a central database rather than in individual routers. TACACS+ also provides support for separate modular authentication, authorization, and accounting (AAA) facilities that are configured at individual routers.

Network Interfaces

This section describes the network interface protocols that Cisco 860 and Cisco 880 series routers support. The following network interface protocols are supported:

- Ethernet
- ATM for DSL

Ethernet

Ethernet is a baseband LAN protocol that transports data and voice packets to the WAN interface using carrier sense multiple access collision detect (CSMA/CD). The term is now often used to refer to all CSMA/CD LANs. Ethernet was designed to serve in networks with sporadic, occasionally heavy traffic requirements. The IEEE 802.3 specification was developed in 1980, based on the original Ethernet technology.

Under the Ethernet CSMA/CD media-access process, any host on a CSMA/CD LAN can access the network at any time. Before sending data, CSMA/CD hosts listen for traffic on the network. A host wanting to send data waits until it detects no traffic before it transmits. Ethernet allows any host on the network to transmit whenever the network is quiet. A collision occurs when two hosts listen for traffic, hear none, and then transmit simultaneously. In this situation, both transmissions are damaged, and the hosts must retransmit at some later time. Algorithms determine when the colliding hosts should retransmit.

ATM for DSL

Asynchronous Transfer Mode (ATM) is a high-speed multiplexing and switching protocol that supports multiple traffic types, including voice, data, video, and imaging.

ATM is composed of fixed-length cells that switch and multiplex all information for the network. An ATM connection is simply used to transfer bits of information to a destination router or host. The ATM network is considered a LAN with high bandwidth availability. Unlike a LAN, which is connectionless, ATM requires certain features to provide a LAN environment to the users.

Each ATM node must establish a separate connection to every node in the ATM network that it needs to communicate with. All such connections are established through a permanent virtual circuit (PVC).

PVC

A PVC is a connection between remote hosts and routers. A PVC is established for each ATM end node with which the router communicates. The characteristics of the PVC that are established when it is created are set by the ATM adaptation layer (AAL) and the encapsulation type. An AAL defines the conversion of user information into cells. An AAL segments upper-layer information into cells at the transmitter and reassembles the cells at the receiver.

Cisco routers support the AAL5 format, which provides a streamlined data transport service that functions with less overhead and affords better error detection and correction capabilities than AAL3/4. AAL5 is typically associated with variable bit rate (VBR) traffic and unspecified bit rate (UBR) traffic.

ATM encapsulation is the wrapping of data in a particular protocol header. The type of router that you are connecting to determines the type of ATM PVC encapsulation.

The routers support the following encapsulation types for ATM PVCs:

- LLC/SNAP (RFC 1483)
- VC-MUX (RFC 1483)
- PPP (RFC 2364)

Each PVC is considered a complete and separate link to a destination node. Users can encapsulate data as needed across the connection. The ATM network disregards the contents of the data. The only requirement is that data be sent to the ATM subsystem of the router in a manner that follows the specific AAL format.

Dialer Interface

A dialer interface assigns PPP features (such as authentication and IP address assignment method) to a PVC. Dialer interfaces are used when configuring PPP over ATM.

Dialer interfaces can be configured independently of any physical interface and applied dynamically as needed.

Dial Backup

Dial backup provides protection against WAN downtime by allowing a user to configure a backup modem line connection. The following can be used to bring up the dial backup feature in Cisco IOS software:

- Backup Interface
- Floating Static Routes
- Dialer Watch

Backup Interface

A backup interface is an interface that stays idle until certain circumstances occur, such as WAN downtime, at which point it is activated. The backup interface can be a physical interface such as a Basic Rate Interface (BRI), or an assigned backup dialer interface to be used in a dialer pool. While the primary line is up, the backup interface is placed in standby mode. In standby mode, the backup interface is effectively shut down until it is enabled. Any route associated with the backup interface does not appear in the routing table.

Because the backup interface command is dependent on the router's identifying that an interface is physically down, it is commonly used to back up ISDN BRI connections, asynchronous lines, and leased lines. The interfaces to such connections go down when the primary line fails, and the backup interface quickly identifies such failures.

Floating Static Routes

Floating static routes are static routes that have an administrative distance greater than the administrative distance of dynamic routes. Administrative distances can be configured on a static route so that the static route is less desirable than a dynamic route. In this manner, the static route is not used when the dynamic route is available. However, if the dynamic route is lost, the static route can take over, and the traffic can be sent through this alternative route. If this alternative route uses a dial-on-demand routing (DDR) interface, then that interface can be used as a backup feature.

Dialer Watch

Dialer watch is a backup feature that integrates dial backup with routing capabilities. Dialer watch provides reliable connectivity without having to define traffic of interest to trigger outgoing calls at the central router. Hence, dialer watch can be considered regular DDR with no requirement for traffic of interest. By configuring a set of watched routes that define the primary interface, you can monitor and track the status of the primary interface as watched routes are added and deleted.

When a watched route is deleted, dialer watch checks for at least one valid route for any of the IP addresses or networks being watched. If there is no valid route, the primary line is considered down and unusable. If there is a valid route for at least one of the watched IP networks defined and the route is pointing to an interface other than the backup interface configured for dialer watch, the primary link is considered up and dialer watch does not initiate the backup link.

NAT

Network Address Translation (NAT) provides a mechanism for a privately addressed network to access registered networks, such as the Internet, without requiring a registered subnet address. This mechanism eliminates the need for host renumbering and allows the same IP address range to be used in multiple intranets.

NAT is configured on the router at the border of an *inside network* (a network that uses nonregistered IP addresses) and an *outside network* (a network that uses a globally unique IP address; in this case, the Internet). NAT translates the inside local addresses (the nonregistered IP addresses assigned to hosts on the inside network) into globally unique IP addresses before sending packets to the outside network.

With NAT, the inside network continues to use its existing private or obsolete addresses. These addresses are converted into legal addresses before packets are forwarded onto the outside network. The translation function is compatible with standard routing; the feature is required only on the router connecting the inside network to the outside domain.

Translations can be static or dynamic. A static address translation establishes a one-to-one mapping between the inside network and the outside domain. Dynamic address translations are defined by describing the local addresses to be translated and the pool of addresses from which to allocate outside addresses. Allocation occurs in numeric order, and multiple pools of contiguous address blocks can be defined.

NAT eliminates the need to readdress all hosts that require external access, saving time and money. It also conserves addresses through application port-level multiplexing. With NAT, internal hosts can share a single registered IP address for all external communications. In this type of configuration, relatively few external addresses are required to support many internal hosts, thus conserving IP addresses.

Because the addressing scheme on the inside network may conflict with registered addresses already assigned within the Internet, NAT can support a separate address pool for overlapping networks and translate as appropriate.

Easy IP (Phase 1)

The Easy IP (Phase 1) feature combines Network Address Translation (NAT) and PPP/Internet Protocol Control Protocol (IPCP). This feature enables a Cisco router to automatically negotiate its own registered WAN interface IP address from a central server and to enable all remote hosts to access the Internet using this single registered IP address. Because Easy IP (Phase 1) uses existing port-level multiplexed NAT functionality within Cisco IOS software, IP addresses on the remote LAN are invisible to the Internet.

The Easy IP (Phase 1) feature combines NAT and PPP/IPCP. With NAT, the router translates the nonregistered IP addresses used by the LAN devices into the globally unique IP address used by the dialer interface. The ability of multiple LAN devices to use the same globally unique IP address is known as *overloading*. NAT is configured on the router at the border of an inside network (a network that uses nonregistered IP addresses) and an outside network (a network that uses a globally unique IP address; in this case, the Internet).

With PPP/IPCP, Cisco routers automatically negotiate a globally unique (registered) IP address for the dialer interface from the ISP router.

Easy IP (Phase 2)

The Easy IP (Phase 2) feature combines Dynamic Host Configuration Protocol (DHCP) server and relay. DHCP is a client-server protocol that enables devices on an IP network (the DHCP clients) to request configuration information from a DHCP server. DHCP allocates network addresses from a central pool on an as-needed basis. DHCP is useful for assigning IP addresses to hosts that are temporarily connected to the network or for sharing a limited pool of IP addresses among a group of hosts that do not need permanent IP addresses.

DHCP frees you from having to assign an IP address to each client manually.

DHCP configures the router to forward User Datagram Protocol (UDP) broadcasts, including IP address requests, from DHCP clients. DHCP allows for increased automation and fewer network administration problems by:

- Eliminating the need for the manual configuration of individual computers, printers, and shared file systems
- Preventing the simultaneous use of the same IP address by two clients
- Allowing configuration from a central site

QoS

This section describes quality of service (QoS) parameters, including the following:

- IP Precedence
- PPP Fragmentation and Interleaving
- CBWFQ
- RSVP
- Low Latency Queuing

QoS refers to the capability of a network to provide better service to selected network traffic over various technologies, including ATM, Ethernet and IEEE 802.1 networks, and IP-routed networks that may use any or all of these underlying technologies. Primary goals of QoS include dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. QoS technologies provide the elemental building blocks for future business applications in campus, WAN, and service provider networks.

QoS must be configured throughout your network, not just on your router running VoIP, to improve voice network performance. Not all QoS techniques are appropriate for all network routers. Edge routers and backbone routers in your network do not necessarily perform the same operations; the QoS tasks they perform might differ as well. To configure your IP network for real-time voice traffic, you need to consider the functions of both edge and backbone routers in your network.

QoS software enables complex networks to control and predictably service a variety of networked applications and traffic types. Almost any network can take advantage of QoS for optimum efficiency, whether it is a small corporate network, an Internet service provider, or an enterprise network.

IP Precedence

You can partition traffic in up to six classes of service using IP Precedence (two others classes are reserved for internal network use). The queuing technologies throughout the network can then use this signal to expedite handling.

Features such as policy-based routing and committed access rate (CAR) can be used to set precedence based on extended access-list classification. This allows considerable flexibility for precedence assignment, including assignment by application or user, by destination and source subnet, and so on. Typically this functionality is deployed as close to the edge of the network (or administrative domain) as possible, so that each subsequent network element can provide service based on the determined policy.

IP Precedence can also be set in the host or network client with the signaling used optionally. IP Precedence enables service classes to be established using existing network queuing mechanisms (such as class-based weighted fair queueing [CBWFQ]) with no changes to existing applications or complicated network requirements.

PPP Fragmentation and Interleaving

With multiclass multilink PPP interleaving, large packets can be multilink-encapsulated and fragmented into smaller packets to satisfy the delay requirements of real-time voice traffic; small real-time packets, which are not multilink encapsulated, are transmitted between fragments of the large packets. The interleaving feature also provides a special transmit queue for the smaller, delay-sensitive packets, enabling them to be transmitted earlier than other flows. Interleaving provides the delay bounds for delay-sensitive voice packets on a slow link that is used for other best-effort traffic.

In general, multilink PPP with interleaving is used in conjunction with CBWFQ and RSVP or IP Precedence to ensure voice packet delivery. Use multilink PPP with interleaving and CBWFQ to define how data is managed; use Resource Reservation Protocol (RSVP) or IP Precedence to give priority to voice packets.

CBWFQ

In general, class-based weighted fair queuing (CBWFQ) is used in conjunction with multilink PPP and interleaving and RSVP or IP Precedence to ensure voice packet delivery. CBWFQ is used with multilink PPP to define how data is managed; RSVP or IP Precedence is used to give priority to voice packets.

There are two levels of queuing; ATM queues and Cisco IOS queues. CBWFQ is applied to Cisco IOS queues. A first-in-first-out (FIFO) Cisco IOS queue is automatically created when a PVC is created. If you use CBWFQ to create classes and attach them to a PVC, a queue is created for each class.

CBWFQ ensures that queues have sufficient bandwidth and that traffic gets predictable service. Low-volume traffic streams are preferred; high-volume traffic streams share the remaining capacity, obtaining equal or proportional bandwidth.

RSVP

RSVP enables routers to reserve enough bandwidth on an interface to ensure reliability and quality performance. RSVP allows end systems to request a particular QoS from the network. Real-time voice traffic requires network consistency. Without consistent QoS, real-time traffic can experience jitter, insufficient bandwidth, delay variations, or information loss. RSVP works in conjunction with current queuing mechanisms. It is up to the interface queuing mechanism (such as CBWFQ) to implement the reservation.

RSVP works well on PPP, HDLC, and similar serial-line interfaces. It does not work well on multi-access LANs. RSVP can be equated to a dynamic access list for packet flows.

You should configure RSVP to ensure QoS if the following conditions describe your network:

- Small-scale voice network implementation
- Links slower than 2 Mbps
- Links with high utilization
- Need for the best possible voice quality

Low Latency Queuing

Low latency queuing (LLQ) provides a low-latency strict priority transmit queue for real-time traffic. Strict priority queuing allows delay-sensitive data to be dequeued and sent first (before packets in other queues are dequeued), giving delay-sensitive data preferential treatment over other traffic.

Access Lists

With basic standard and static extended access lists, you can approximate session filtering by using the established keyword with the **permit** command. The established keyword filters TCP packets based on whether the ACK or RST bits are set. (Set ACK or RST bits indicate that the packet is not the first in the session and the packet therefore belongs to an established session.) This filter criterion would be part of an access list applied permanently to an interface.

APPENDIX C

ROM Monitor

The ROM monitor firmware runs when the router is powered up or reset. The firmware helps to initialize the processor hardware and boot the operating system software. You can use the ROM monitor to perform certain configuration tasks, such as recovering a lost password or downloading software over the console port. If there is no Cisco IOS software image loaded on the router, the ROM monitor runs the router.

This appendix contains the following sections:

- Entering the ROM Monitor, page C-1
- ROM Monitor Commands, page C-2
- Command Descriptions, page C-3
- Disaster Recovery with TFTP Download, page C-4
- Configuration Register, page C-6
- Console Download, page C-7
- Debug Commands, page C-9
- Exiting the ROM Monitor, page C-10

Entering the ROM Monitor

To use the ROM monitor, you must be using a terminal or PC that is connected to the router over the console port.

Perform these steps to configure the router to boot up in ROM monitor mode the next time it is rebooted.

	Command	Purpose
Step 1	**enable**	Enters privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal**	Enters global configuration mode.
Step 3	**config-reg 0x0**	Resets the configuration register.

	Command	Purpose
Step 4	**exit**	Exits global configuration mode.
Step 5	**reload**	Reboots the router with the new configuration register value. The router remains in ROM monitor and does not boot the Cisco IOS software. As long as the configuration value is 0x0, you must manually boot the operating system from the console. See the **boot** command in the "Command Descriptions" section in this appendix. After the router reboots, it is in ROM monitor mode. The number in the prompt increments with each new line.

Timesaver Break (system interrupt) is always enabled for 60 seconds after the router reboots, regardless of whether it is set to on or off in the configuration register. During this 60-second window, you can break to the ROM monitor prompt by pressing the Break key.

ROM Monitor Commands

Enter **?** or **help** at the ROM monitor prompt to display a list of available commands and options, as follows:

```
rommon 1 > ?
alias                  set and display aliases command
boot                   boot up an external process
break                  set/show/clear the breakpoint
confreg                configuration register utility
cont                   continue executing a downloaded image
context                display the context of a loaded image
cookie                 display contents of cookie PROM in hex
copy                   Copy a file-copy [-b <buffer_size>] <src_file> <dst_file>
delete                 Delete file(s)-delete <filenames ...>
dir                    List files in directories-dir <directory>
dis                    display instruction stream
dnld                   serial download a program module
format                 Format a filesystem-format <filessystem>
frame                  print out a selected stack frame
fsck                   Check filesystem consistency-fsck <filesystem>
help                   monitor builtin command help
history                monitor command history
meminfo                main memory information
mkdir                  Create dir(s)-mkdir <dirnames ...>
more                   Concatenate (type) file(s)-cat <filenames ...>
rename                 Rename a file-rename <old_name> <new_name>
repeat                 repeat a monitor command
reset                  system reset
rmdir                  Remove a directory
set                    display the monitor variables
stack                  produce a stack trace
sync                   write monitor environment to NVRAM
sysret                 print out info from last system return
tftpdnld               tftp image download
unalias                unset an alias
unset                  unset a monitor variable
xmodem                 x/ymodem image download
```

ROM Monitor Commands for 860VAE ISRs

Cisco 866VAE, 867VAE, 866VAE-K9, and 867VAE-K9 ISRs support the following ROM monitor commands. Enter **?** or **help** at the ROM monitor prompt to display a list of available commands and options, as follows:

```
rommon 1 > ?
alias                  set and display aliases command
boot                   boot up an external process
confreg                configuration register utility
delete                 Delete file(s)-delete <filenames ...>
dev                    List the device table
dir                    List files in directories-dir <directory>
format                 Format a filesystem-format <filessystem>
help                   monitor builtin command help
history                monitor command history
meminfo                main memory information
repeat                 repeat a monitor command
reset                  system reset
set                    display the monitor variables
showmon                display currently selected ROM monitor
sync                   write monitor environment to NVRAM
tftpdnld               tftp image download
unalias                unset an alias
unset                  unset a monitor variable
```

Commands are case sensitive. You can halt any command by pressing the Break key on a terminal. If you are using a PC, most terminal emulation programs halt a command when you press the Ctrl and the Break keys at the same time. If you are using another type of terminal emulator or terminal emulation software, see the documentation for that product for information on how to send a Break command.

Command Descriptions

Table C-1 describes the most commonly used ROM monitor commands.

Table C-1 Commonly Used ROM Monitor Commands

Command	Description
help or **?**	Displays a summary of all available ROM monitor commands.

-?	Displays information about command syntax; for example:
	`rommon 16 > dis -?`
	`usage : dis [addr] [length]`
	The output for this command is slightly different for the **xmodem** download command:
	`rommon 11 > xmodem -?`
	`xmodem: illegal option -- ?`
	`usage: xmodem [-cyrxu] <destination filename>`
	`-c  CRC-16`
	`-y  ymodem-batch protocol`
	`-r  copy image to dram for launch`
	`-x  do not launch on download completion`
	`-u  upgrade ROMMON, System will reboot after upgrade`

reset or **i**	Resets and initializes the router, similar to a power up.

Table C-1 Commonly Used ROM Monitor Commands (continued)

Command	Description

dir *device***:**	Lists the files on the named device; for example, flash memory files:
	`rommon 4 > dir flash:`
	`Directory of flash:/`
	`2 -rwx 10283208 <date> c880-advsecurityk9-mz`
	`9064448 bytes available (10289152 bytes used)`

boot commands	For more information about the ROM monitor boot commands, see the *Cisco IOS Configuration Fundamentals and Network Management Guide*.
b	Boots the first image in flash memory.
b flash: [*filename*]	Attempts to boot the image directly from the first partition of flash memory. If you do not enter a filename, this command will boot this first image in flash memory.

Disaster Recovery with TFTP Download

The standard way to load new software on your router is to use the **copy tftp flash** privileged EXEC command from the Cisco IOS software command-line interface (CLI). However, if the router is unable to boot Cisco IOS software, you can load new software while in ROM monitor mode.

This section describes how to load a Cisco IOS software image from a remote TFTP server to the router flash memory. Use the **tftpdnld** command only for disaster recovery, because it erases all existing data in flash memory before downloading a new software image to the router.

TFTP Download Command Variables

This section describes the system variables that can be set in ROM monitor mode and that are used during the TFTP download process. There are both required variables and optional variables.

Note The commands described in this section are case sensitive and must be entered exactly as shown.

Required Variables

These variables must be set with these commands before you use the **tftpdnld** command:

Variable	Command
IP address of the router.	**IP_ADDRESS=** *ip_address*
Subnet mask of the router.	**IP_SUBNET_MASK=** *ip_address*
IP address of the default gateway of the router.	**DEFAULT_GATEWAY=** *ip_address*

IP address of the TFTP server from which the software will be downloaded.	**TFTP_SERVER=** *ip_address*
Name of the file that will be downloaded to the router.	**TFTP_FILE=** *filename*

Optional Variables

These variables can be set with these commands before using the **tftpdnld** command:

Variable	Command
Configures how the router displays file download progress. 0—No progress is displayed. 1—Exclamation points (!!!) are displayed to indicate file download progress. This is the default setting. 2—Detailed progress is displayed during the file download process; for example: • Initializing interface. • Interface link state up. • ARPing for 1.4.0.1 • ARP reply for 1.4.0.1 received. MAC address 00:00:0c:07:ac:01	**TFTP_VERBOSE=** *setting*
Number of times the router attempts ARP and TFTP download. The default is 7.	**TFTP_RETRY_COUNT=** *retry_times*
Length of time, in seconds, before the download process times out. The default is 2,400 seconds (40 minutes).	**TFTP_TIMEOUT=** *time*
Whether or not the router performs a checksum test on the downloaded image: 1—Checksum test is performed. 0—No checksum test is performed.	**TFTP_CHECKSUM=***setting*

Using the TFTP Download Command

To download a file through TFTP perform these steps in ROM monitor mode

Step 1 Use the appropriate commands to enter all the required variables and any optional variables described in preceding sections.

Step 2 Enter the **tftpdnld** command as follows:

```
rommon 1 > tftpdnld -r
```

Note The **-r** variable is optional. Entering this variable downloads and boots the new software but does not save the software to flash memory. You can then use the image that is in flash memory the next time you enter the **reload** command.

You will see output similar to the following:

```
IP_ADDRESS: 10.3.6.7
IP_SUBNET_MASK: 255.255.0.0
DEFAULT_GATEWAY: 10.3.0.1
TFTP_SERVER: 192.168.254.254
TFTP_FILE: c880-advsecurityk9-mz
Do you wish to continue? y/n:  [n]:
```

Step 3 If you are sure that you want to continue, enter **y** in response to the question in the output:

```
Do you wish to continue? y/n:  [n]:y
```

The router begins to download the new file.

If you mistakenly entered yes, you can enter **Ctrl-C** or **Break** to stop the transfer before the flash memory is erased.

Configuration Register

The virtual configuration register is in nonvolatile RAM (NVRAM) and has the same functionality as other Cisco routers. You can view or modify the virtual configuration register from either the ROM monitor or the operating system software. Within the ROM monitor, you can change the configuration register by entering the register value in hexadecimal format, or by allowing the ROM monitor to prompt you for the setting of each bit.

Changing the Configuration Register Manually

To change the virtual configuration register from the ROM monitor manually, enter the **confreg** command followed by the new value of the register in hexadecimal format, as shown in the following example:

```
rommon 1 > confreg 0x2101


You must reset or power cycle for new config to take effect
rommon 2 >
```

The value is always interpreted as hexadecimal. The new virtual configuration register value is written into NVRAM but does not take effect until you reset or reboot the router.

Changing the Configuration Register Using Prompts

Entering the **confreg** command without an argument displays the contents of the virtual configuration register and a prompt to alter the contents by describing the meaning of each bit.

In either case, the new virtual configuration register value is written into NVRAM but does not take effect until you reset or reboot the router.

The following display shows an example of entering the **confreg** command:

```
rommon 7> confreg

     Configuration Summary
enabled are:
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:  y
enable  “diagnostic mode”? y/n  [n]:  y
enable  “use net in IP bcast address”? y/n  [n]:
enable  “load rom after netboot fails”? y/n  [n]:
enable  “use all zero broadcast”? y/n  [n]:
enable  “break/abort has effect”? y/n  [n]:
enable  “ignore system config info”? y/n  [n]:
change console baud rate? y/n  [n]:  y
enter rate: 0 = 9600, 1 = 4800, 2 = 1200, 3 = 2400  [0]:  0
change the boot characteristics? y/n  [n]:  y
enter to boot:
 0 = ROM Monitor
 1 = the boot helper image
 2-15 = boot system
    [0]:  0

Configuration Summary
enabled are:
diagnostic mode
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:


You must reset or power cycle for new config to take effect
```

Console Download

You can use console download, which is a ROM monitor function, to download either a software image or a configuration file over the router console port. After download, the file is either saved to the mini-flash memory module or to main memory for execution (image files only).

Use console download when you do not have access to a TFTP server.

Note If you want to download a software image or a configuration file to the router over the console port, you must use the ROM monitor **dnld** command.

Note If you are using a PC to download a Cisco IOS image over the router console port at 115,200 bps, ensure that the PC serial port is using a 16550 universal asynchronous transmitter/receiver (UART). If the PC serial port is not using a 16550 UART, we recommend using a speed of 38,400 bps or less when downloading a Cisco IOS image over the console port.

Command Description

The following are the syntax and descriptions for the **xmodem** console download command:

xmodem [-cyrx] *destination_file_name*

c	Optional. Performs the download using 16-bit cyclic redundancy check (CRC-16) error checking to validate packets. Default is 8-bit CRC.
y	Optional. Sets the router to perform the download using Ymodem protocol. The default is Xmodem protocol. The protocols differ as follows: • Xmodem supports a 128-block transfer size. Ymodem supports a 1024-block transfer size. • Ymodem uses CRC-16 error checking to validate each packet. Depending on the device that the software is being downloaded from, this function might not be supported by Xmodem.
r	Optional. Image is loaded into DRAM for execution. The default is to load the image into flash memory.
x	Optional. Image is loaded into DRAM without being executed.
destination_ file_name	Name of the system image file or the system configuration file. In order for the router to recognize it, the name of the configuration file must be *router_confg*.

Follow these steps to run Xmodem:

Step 1 Move the image file to the local drive where Xmodem will execute.

Step 2 Enter the **xmodem** command.

Error Reporting

Because the ROM monitor console download uses the console to perform the data transfer, when an error occurs during a data transfer, error messages are only displayed on the console once the data transfer is terminated.

If you have changed the baud rate from the default rate, the error message is followed by a message telling you to restore the terminal to the baud rate specified in the configuration register.

Debug Commands

Most ROM monitor debugging commands are functional only when Cisco IOS software has crashed or is halted. If you enter a debugging command and Cisco IOS crash information is not available, you see the following error message:

```
"xxx: kernel context state is invalid, can not proceed."
```

The following are ROM monitor debugging commands:

- **stack** or **k**—Produces a stack trace; for example:

```
rommon 6> stack
Stack trace:
PC = 0x801111b0
Frame 00: FP = 0x80005ea8    PC = 0x801111b0
Frame 01: FP = 0x80005eb4    PC = 0x80113694
Frame 02: FP = 0x80005f74    PC = 0x8010eb44
Frame 03: FP = 0x80005f9c    PC = 0x80008118
Frame 04: FP = 0x80005fac    PC = 0x80008064
Frame 05: FP = 0x80005fc4    PC = 0xfff03d70
```

- **context**—Displays processor context; for example:

```
rommon 7> context
CPU context of the most recent exception:
PC  = 0x801111b0  MSR = 0x00009032  CR  = 0x53000035  LR    = 0x80113694
CTR = 0x801065e4  XER = 0xa0006d36  DAR = 0xffffffff  DSISR = 0xffffffff
DEC = 0xffffffff  TBU = 0xffffffff  TBL = 0xffffffff  IMMR  = 0xffffffff
R0  = 0x00000000  R1  = 0x80005ea8  R2  = 0xffffffff  R3    = 0x00000000
R4  = 0x8fab0d76  R5  = 0x80657d00  R6  = 0x80570000  R7    = 0x80570000
R8  = 0x00000000  R9  = 0x80570000  R10 = 0x0000954c  R11   = 0x00000000
R12 = 0x00000080  R13 = 0xffffffff  R14 = 0xffffffff  R15   = 0xffffffff
R16 = 0xffffffff  R17 = 0xffffffff  R18 = 0xffffffff  R19   = 0xffffffff
R20 = 0xffffffff  R21 = 0xffffffff  R22 = 0xffffffff  R23   = 0xffffffff
R24 = 0xffffffff  R25 = 0xffffffff  R26 = 0xffffffff  R27   = 0xffffffff
R28 = 0xffffffff  R29 = 0xffffffff  R30 = 0xffffffff  R31   = 0xffffffff
```

- **frame**—Displays an individual stack frame.
- **sysret**—Displays return information from the last booted system image. This information includes the reason for terminating the image, a stack dump of up to eight frames, and, if an exception is involved, the address where the exception occurred; for example:

```
rommon 8> sysret
System Return Info:
count: 19,  reason: user break
pc:0x801111b0,  error address: 0x801111b0
Stack Trace:
FP: 0x80005ea8, PC: 0x801111b0
FP: 0x80005eb4, PC: 0x80113694
FP: 0x80005f74, PC: 0x8010eb44
FP: 0x80005f9c, PC: 0x80008118
FP: 0x80005fac, PC: 0x80008064
FP: 0x80005fc4, PC: 0xfff03d70
FP: 0x80005ffc, PC: 0x00000000
FP: 0x00000000, PC: 0x00000000
```

- **meminfo**—Displays size in bytes, starting address, available range of main memory, the starting point and size of packet memory, and size of NVRAM; for example:

```
rommon 9> meminfo
Main memory size: 40 MB.
Available main memory starts at 0x10000, size 40896KB
```

```
IO (packet) memory size: 5 percent of main memory.
NVRAM size: 32KB
```

Exiting the ROM Monitor

You must set the configuration register to a value from 0x2 to 0xF for the router to boot a Cisco IOS image from flash memory upon startup or reloading.

The following example shows how to reset the configuration register and cause the router to boot a Cisco IOS image stored in flash memory:

```
rommon 1 > confreg 0x2101
```

You must reset or power cycle for new config to take effect:

```
rommon 2 > boot
```

The router will boot the Cisco IOS image in flash memory. The configuration register will change to 0x2101 the next time the router is reset or power cycled.

APPENDIX D

Common Port Assignments

Table D-1 lists currently assigned Transmission Control Protocol (TCP) port numbers. To the extent possible, the User Datagram Protocol (UDP) uses the same numbers.

Table D-1 Currently Assigned TCP and UDP Port Numbers

Port	Keyword	Description
0	—	Reserved
1–4	—	Unassigned
5	RJE	Remote job entry
7	ECHO	Echo
9	DISCARD	Discard
11	USERS	Active users
13	DAYTIME	Daytime
15	NETSTAT	Who is up or NETSTAT
17	QUOTE	Quote of the day
19	CHARGEN	Character generator
20	FTP-DATA	File Transfer Protocol (data)
21	FTP	File Transfer Protocol
23	TELNET	Terminal connection
25	SMTP	Simple Mail Transport Protocol
37	TIME	Time
39	RLP	Resource Location Protocol
42	NAMESERVER	Hostname server
43	NICNAME	Who is
49	LOGIN	Login Host Protocol
53	DOMAIN	Domain name server
67	BOOTPS	Bootstrap Protocol Server
68	BOOTPC	Bootstrap Protocol Client
69	TFTP	Trivial File Transfer Protocol
75	—	Any private dial-out service

Table D-1 Currently Assigned TCP and UDP Port Numbers (continued)

Port	Keyword	Description
77	—	Any private RJE service
79	FINGER	Finger
95	SUPDUP	SUPDUP Protocol
101	HOST NAME	Network interface card (NIC) hostname server
102	ISO-TSAP	ISO-Transport Service Access Point (TSAP)
103	X400	X400
104	X400-SND	X400-SND
111	SUNRPC	Sun Microsystems Remote Procedure Call
113	AUTH	Authentication service
117	UUCP-PATH	UNIX-to-UNIX Copy Protocol (UUCP) Path Service
119	NNTP	Usenet Network News Transfer Protocol
123	NTP	Network Time Protocol
126	SNMP	Simple Network Management Protocol
137	NETBIOS-NS	NetBIOS name service
138	NETBIOS-DGM	NetBIOS datagram service
139	NETBIOS-SSN	NetBIOS session service
161	SNMP	Simple Network Management Protocol
162	SNMP-TRAP	Simple Network Management Protocol traps
512	rexec	UNIX remote execution (control)
513	TCP—rlogin UDP—rwho	TCP—UNIX remote login UDP—UNIX broadcast name service
514	TCP—rsh UDP—syslog	TCP—UNIX remote shell UDP—system log
515	Printer	UNIX line printer remote spooling
520	RIP	Routing Information Protocol
525	Timed	Time server