# Cisco Reader Comment Card

## General Information

**1** Years of networking experience: ______ Years of experience with Cisco products: ______

**2** I have these network types: □ LAN □ Backbone □ WAN
□ Other: ____________________

**3** I have these Cisco products: □ Switches □ Routers
□ Other (specify models): ____________________

**4** I perform these types of tasks: □ H/W installation and/or maintenance □ S/W configuration
□ Network management □ Other: ____________________

**5** I use these types of documentation: □ H/W installation □ H/W configuration □ S/W configuration
□ Command reference □ Quick reference □ Release notes □ Online help
□ Other: ____________________

**6** I access this information through: ____% Cisco.com (CCO) ____% CD-ROM
____% Printed docs ____% Other: ____________________

**7** I prefer this access method: ____________________

**8** I use the following three product features the most:
____________________
____________________
____________________

## Document Information

Document Title: Cisco 800 Series Software Configuration Guide

Part Number: 78-5372-06 S/W Release (if applicable): 12.2(8)YN

On a scale of 1–5 (5 being the best), please let us know how we rate in the following areas:

______ The document is written at my technical level of understanding.

______ The document is complete.

______ The information is well organized.

______ The information is accurate.

______ The information I wanted was easy to find.

______ The information I found was useful to my job.

Please comment on our lowest scores:
____________________
____________________
____________________
____________________

## Mailing Information

Company Name Date

Contact Name Job Title

Mailing Address

____________________

City State/Province ZIP/Postal Code

Country Phone (  ) Extension

Fax (  ) E-mail

Can we contact you further concerning our documentation? □ Yes □ No

You can also send us your comments by e-mail to **bug-doc@cisco.com**, or by fax to **408-527-8089**.

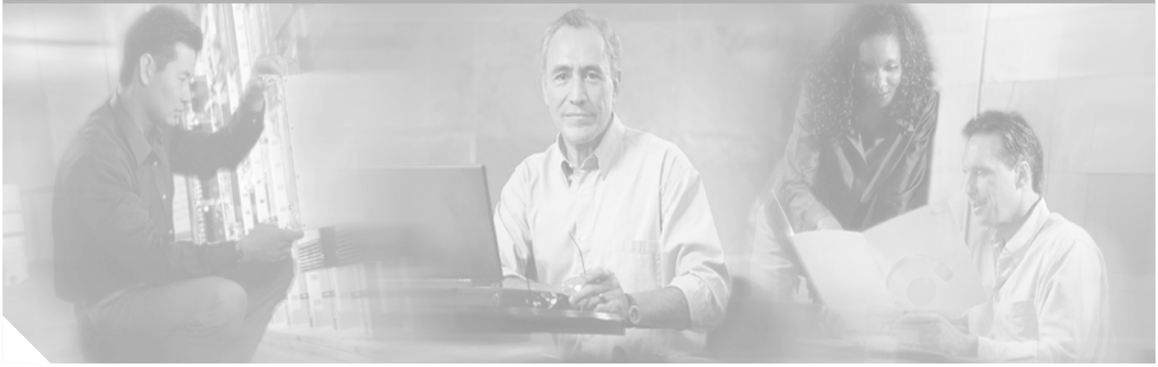
NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

**BUSINESS REPLY MAIL**

FIRST-CLASS MAIL PERMIT NO. 4631 SAN JOSE CA

POSTAGE WILL BE PAID BY ADDRESSEE

DOCUMENT RESOURCE CONNECTION
CISCO SYSTEMS INC
170 WEST TASMAN DR
SAN JOSE CA 95134-9916



# Cisco 800 Series Software Configuration Guide

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-785372=
Text Part Number: 78-5372-06

*Cisco 800 Series Software Configuration Guide*

# CONTENTS

# About This Guide

This preface describes the audience for, organization of, and conventions used in this guide. It also provides information on how to access this guide and other Cisco documentation on the Documentation CD-ROM that ships with Cisco routers and is available on the World Wide Web.

This document provides software configuration information for the following Cisco routers:

- Cisco 801, 802, 803, 804, 811, and 813 ISDN routers
- Cisco 805 serial interface router
- Cisco 806 Ethernet router
- Cisco 820 series routers
- Cisco 831, 836, and 837 routers
- Cisco SOHO 70 series routers
- Cisco SOHO 91, 96, and 97 routers

# Audience

This guide is intended for network administrators whose backgrounds vary from having no or little experience configuring routers to having a high level of experience. You can use this guide in the following ways:

- You have configured the software using the Cisco Router Web Setup tool, and want to configure additional advanced software features using the command-line interface (CLI).
- You want to configure the software using only the CLI.

**Note** Cisco recommends that inexperienced network administrators use the Cisco Router Web Setup tool to configure their routers.

See the "Organization" section of this guide to help you find the chapter(s) containing the information you need to configure your software.

# Organization

This guide contains the following information:

- Chapter 1, "Concepts"—Provides general concept explanations of the Cisco 800 series and Cisco SOHO routers.
- Chapter 2, "Configuring Basic Networks"—Describes three basic networks that are appropriate to small independent offices and/or telecommuters.
- Chapter 3, "Configuring Advanced Networks"—Presents more advanced network scenarios involving a private IP network to the Internet and a corporate network, and a remote network to two corporate networks.
- Chapter 4, "Network Scenarios"—Describes five Internet access scenarios and one voice scenario with their specific network topologies and configurations.
- Chapter 5, "Configuring Remote CAPI"—Describes the Remote Common Application Programming Interface (CAPI), a PC-based application programming interface standard used to access ISDN equipment.

- Chapter 6, "Configuring Telephone Interfaces"—Describes how to configure standard and advanced features for the Cisco 800 series routers that support telephone features.
- Chapter 7, "Router Feature Configuration"—Explains basic router configuration, feature by feature.
- Chapter 8, "Advanced Router Configuration"—Explains advanced router configuration features.
- Chapter 9, "Troubleshooting"—Provides information on identifying and solving problems with the ADSL line and the telephone interface. Also explains how to recover a lost software password.
- Appendix A, "Cisco IOS Basic Skills"—Explains what you need to know about the Cisco IOS software before you begin to configure it.
- Appendix B, "ROM Monitor"—Describes the use of the ROM Monitor (ROMMON) utility.
- Appendix C, "Common Port Assignments"—Describes the currently assigned Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) port numbers.
- Appendix D, "Provisioning an ISDN Line"—Describes ISDN lines and switches and the features available, and tells how to order an ISDN line.
- Appendix E, "ISDN BRI Cause Values"—Describes ISDN BRI standard cause values that might be received from the ISDN switch to indicate ISDN call status.

# Conventions

This guide uses the following conventions for instructions and information.

## Notes, Cautions, and Timesavers

Notes, cautions, and time-saving tips use the following conventions and symbols.

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

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

**Timesaver** This symbol means *the described action saves time*.

# Command Conventions

Table 1 describes the command syntax used in this document.

***Table 1 Conventions***

| Convention | Description |
|---|---|
| **boldface** | Commands and keywords. |
| *italic* | Command input that is supplied by you. |
| [ ] | Optional keywords and default responses to system prompts appear within square brackets. |
| {**x** \| **x** \| **x**} | A choice of keywords (represented by **x**) appears in braces separated by vertical bars. You must select one. |
| ^ or Ctrl | Represent the key labeled *Control*. For example, when you read ^*D* or *Ctrl-D*, you should hold down the Control key while you press the D key. |
| `screen font` | Examples of information displayed on the screen. |
| **`boldface screen font`** | Examples of information that you must enter. |

# Related Documents

The following publications provide related information on these products:

- Cisco 800 series routers
  - *Cisco 800 Series Router Cabling and Setup Quick Start Guide*—Provides quick installation information on the Cisco 801–804 routers.
  - *Cisco 800 Series Routers Hardware Installation Guide*—Provides installation information on the Cisco 801–804 routers.
- Cisco 805 router
  - *Cisco 805 Router Cabling and Setup Quick Start Guide*—Provides quick installation information on the Cisco 805 router.
  - *Cisco 805 Router Hardware Installation Guide*—Provides installation information on the Cisco 805 router.
- Cisco 806 router
  - *Cisco 806 Router Cabling and Setup Quick Start Guide*—Provides quick installation information on the Cisco 806 router.
  - *Cisco 806 Router Hardware Installation Guide*—Provides installation information on the Cisco 806 router.
- Cisco 811 and 813 routers
  - *Cisco 811 and 813 Router Cabling and Setup Quick Start Guide*—Provides quick installation information on the Cisco 811 and 813 routers.
  - *Cisco 811 and 813 Router Hardware Installation Guide*—Provides installation information on the Cisco 806 router.
- Cisco 826 router
  - *Cisco 826 Routers Hardware Installation Guide*—Provides installation information on the Cisco 826 routers.
  - *Cisco 826 and Cisco SOHO 76 Router Quick Start Guide*—Provides quick installation information on the Cisco 826 router.

- Cisco 827 router
  - *Cisco 827 Routers Hardware Installation Guide*—Provides installation information on the Cisco 827 routers.
  - *Cisco 827 Router Cabling and Setup Quick Start Guide*—Provides quick installation information on the Cisco 827 routers.
- Cisco 828 and Cisco SOHO 78 routers
  - *Cisco 828 and SOHO 78 Cabling and Setup Quick Start Guide*—Provides quick installation information on the Cisco 828 and Cisco SOHO 78 routers.
  - *Cisco 828 and SOHO 78 Routers Hardware Installation Guide*—Provides installation information on the Cisco 828 and Cisco SOHO 78 routers.
- Cisco SOHO 77 router
  - *Configuration Note for Cisco SOHO Series Routers*—Describes software configuration information for the Cisco small office/home office (SOHO) 77 router. For information on hardware installation, refer to the *Cisco 827 Routers Hardware Installation Guide*.
- Cisco 831 and Cisco SOHO 91 routers
  - *Cisco 831 and SOHO 91 Cabling and Setup Quick Start Guide*—Provides quick installation information on the Cisco 831 and Cisco SOHO 91 routers.
  - *Cisco 831 and SOHO 91 Hardware Installation Guide*—Provides installation information on the Cisco 831 and Cisco SOHO 91 routers.
- Cisco 836 and Cisco SOHO 96 routers
  - *Cisco 836 and SOHO 96 Cabling and Setup Quick Start Guide*—Provides quick installation information on the Cisco 836 and Cisco SOHO 96 routers.
  - *Cisco 831 and SOHO 91 Hardware Installation Guide*—Provides installation information on the Cisco 836 and Cisco SOHO 96 routers.

- Cisco 837 and Cisco SOHO 97 routers
  - *Cisco 837 and SOHO 97 Cabling and Setup Quick Start Guide*—Provides quick installation information on the Cisco 837 and Cisco SOHO 97 routers.
  - *Cisco 837 and SOHO 97 Hardware Installation Guide*—Provides installation information on the Cisco 837 and Cisco SOHO 97 routers.

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.

## References to Cisco IOS Documentation Set

This guide contains several references to the Cisco IOS documentation set. You can access the desired information in the following ways:

- On the Documentation CD-ROM, select **Cisco Product Documentation**, select **Cisco IOS Software Configuration**, click on the IOS release number applicable to your installation. From there, you can browse to and review the alphabetical listings to find the feature.
- On CCO, go to **Software and Support**, and select **Documentation**. Next, select **Cisco Product Documentation**, select **Cisco IOS Software Configuration**, click on the IOS release number applicable to your installation. From there, you can browse to and review the alphabetical listings to find the feature.

# Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

## Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco web sites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

## Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Registered Cisco.com users can order the Documentation CD-ROM (product number DOC-CONDOCCD=) through the online Subscription Store:

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

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Registered Cisco.com users can order the Documentation CD-ROM (Customer Order Number DOC-CONDOCCD=) through the online Subscription Store:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

# Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) Website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

## Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

http://www.cisco.com

## Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The avenue of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.

- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

## Cisco TAC Website

You can use the Cisco TAC website to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://tools.cisco.com/RPF/register/register.do

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

http://www.cisco.com/en/US/support/index.html

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC website so that you can describe the situation in your own words and attach any necessary files.

## Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

# Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco monthly periodical that provides industry professionals with the latest information about the field of networking. You can access *Packet* magazine at this URL:

  http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_packet_magazine.html

- *iQ Magazine* is the Cisco monthly periodical that provides business leaders and decision makers with the latest information about the networking industry. You can access *iQ Magazine* at this URL:

  http://business.cisco.com/prod/tree.taf%3fasset_id=44699&public_view=true&kbns=1.html

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in the design, development, and operation of public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training, with current offerings in network training listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

CHAPTER 1

# Concepts

This chapter contains conceptual information that may be useful to Internet service providers (ISPs) or network administrators when configuring Cisco 800 series and Cisco SOHO series routers. To review some typical network scenarios, see "Network Scenarios" in Chapter 2. For information on specific configurations, see Chapter 7, "Router Feature Configuration," and Chapter 8, "Advanced Router Configuration."

This chapter includes the following topics:

- QoS, page 1-20
- Access Lists, page 1-25

# Overview of Cisco 800 Series and Cisco SOHO Series Routers

The Cisco 801, 802, 803, and 804 routers are Cisco IOS-based members of the Cisco 800 router product line supporting Integrated Services Digital Network (ISDN) connections.

The Cisco 805 router includes one 10BASE-T Ethernet port and one serial port, which can connect EIA/TIA-232, EIA/TIA-449, EIA/TIA-530, EIA/TIA-530A, X.21, and V.35 data terminal equipment (DTE) or data communications equipment (DCE).

The Cisco 806 and Cisco SOHO 71 routers are fixed-configuration IP routers with security features that provide a secure Ethernet gateway for users in small offices, branch offices and home offices using broadband access to the Internet. These routers are designed to work with digital subscriber line (DSL), cable, or long-reach Ethernet (LRE) modems, or with an Ethernet switch serving a multitenant unit. These routers have four 10BASE-T Ethernet ports that function as a hub; the routers also have one 10BASE-T Ethernet WAN port.

The Cisco 811 and 813 routers connect small professional offices or telecommuters over ISDN Basic Rate Interface (BRI) lines to corporate LANs and the Internet. These routers offer multiprotocol routing between LAN and WAN ports. The Cisco 813 router includes the same features as the 811, but adds two telephone ports, and it has four Ethernet ports instead of just one.

The Cisco 826 and 827 and Cisco SOHO 76 and 77 routers are Cisco IOS-based members of the Cisco 800 router family with ATM and Asymmertric Digital Subscriber Line (ADSL) support. Depending on their feature set, the routers send data, voice, and video over high-speed ADSL lines to connect to the Internet or corporate intranets.

The data-only Cisco 826, 827, and 827H routers and the Cisco SOHO 76 and 77 routers have one 10BASE-T Ethernet and one ADSL-over-ISDN or ADSL network port, respectively.

The data-and-voice Cisco 827-4V router has four Foreign Exchange Station (FXS)/plain old telephone service (POTS) ports in addition to the 10BASE-T Ethernet port and one ADSL network port, and it supports Voice over IP (VoIP). The four FXS/POTS ports will support loop-start functions for connecting to POTS devices up to 500 ft. The Cisco 827-4V router includes a digital signal processor (DSP) chip to support VoIP over ATM adaptation layer (AAL5) protocol.

AAL5 operates over the ADSL physical interface for both data and voice. The ADSL protocol supports EOC message sets defined in T1.413 DMT Issue 2 as limited by digital subscriber line access multiplexers (DSLAMs). The ADSL controller and line interface unit are based on Alcatel chip sets.

The Cisco 828 router is Cisco IOS-based with ATM/SHDSL support. The Cisco SOHO 78 router also supports ATM/SHDSL. The routers send data, voice, and video over high-speed G.SHDSL lines to connect to the Internet or corporate intranets.

Both the Cisco 828 router and the Cisco SOHO 78 router provide a 4-port Ethernet hub, in addition to the G.SHDSL port.

Both the Cisco 831 router and the Cisco SOHO 91 Ethernet-to-Ethernet routers can connect a corporate telecommuter or small office to an ISP over a broadband or Ethernet connection to corporate LANs or the Internet. The routers are capable of bridging and multiprotocol routing between LAN and WAN ports. The Cisco 831 router is a hardware encryption–capable router offering business-class features to small offices and enterprise telecommuters. The Cisco SOHO 91 router offers software encryption capability without hardware encryption.

The Cisco 836 and Cisco SOHO 96 routers are ADSL routers with an integrated switch. These routers provide a 4-port Ethernet switch for the LAN and an ADSL physical interface for the WAN compatibility. The Cisco 836 router is a hardware encryption–capable, Ethernet-to-ADSL router offering business-class features to small offices and enterprise telecommuters. The Cisco SOHO 96 router offers software encryption capability without hardware encryption. Both these routers provide an ISDN basic rate interface (BRI) S/T interface as a backup for the ADSL interface.

The Cisco 837 and Cisco SOHO 97 routers are ADSL routers with an integrated switch. These routers provide a 4-port Ethernet switch for LAN and an ADSL physical interface for WAN compatibility. The Cisco 837 router is a hardware encryption–capable, Ethernet-to-ADSL router offering business-class features to small offices and enterprise telecommuters. The Cisco SOHO 97 router offers software encryption capability without hardware encryption.

The Cisco 831, 836, and 837, and Cisco SOHO 91, 96, and 97 routers support switch functions which enable the routers to be connected as a 10/100 BASE-T device. These routers crossover functionality enable them to detect MDI/MDIX to any other PC or hub with a straight-through cable or crossover cable.

Table 1-1 summarizes what interface each Cisco model supports.

*Table 1-1 Interface Supported in Each Cisco Router*

| Interface Supported | Cisco Router Model |
|---|---|
| Ethernet to ISDN | 801, 802, 803, 804 |
| Ethernet to serial (both sync and async) | 805 |
| Ethernet to Ethernet | 806, 831, SOHO 71, SOHO 91 |
| Ethernet to ADSL over ISDN | 826, SOHO 76, 836, SOHO 96 |
| Ethernet to ADSL over POTS | 827, 827H, 827-4V, 837, SOHO 77, SOHO 77H, SOHO 97 |

# ADSL

ADSL is a technology that allows both data and voice to transmit 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 either within a building or campus.

The benefit of ADSL over a serial or dial-up line is that it is always on and always connected, increasing bandwidth and lowering the costs compared with a dial-up or leased line. ADSL technology is asymmetric in that it allows more bandwidth from an NSP’s 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 accessing, 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 reach from central offices and remote terminals to approximately 26,000 feet, 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's central office and a customer site. This symmetry, combined with always-on access (which eliminates call setup), makes SHDSL ideal for LAN access.

# DNS-Based X.25 Routing

X.25 has long operated over an IP network, specifically using Transmission Control Protocol (TCP) as a reliable transport mechanism. This method is known as X.25 over TCP (XOT). However, large networks and financial legacy environments experienced problems with the amount of route configuration that needed to be done manually because each router switching calls over TCP needed to have every destination configured. Every destination from the host router needed a static IP route statement, and for larger environments, there could be as many as several thousand per router. Until now, the only way to map X.121 addresses and IP addresses was on a one-to-one basis using the **x25 route x121address xot ipaddress** command.

The solution to this problem is to centralize route configuration in a single location that routers can then access for their connectivity needs. This centralization is the function of the Domain Name System (DNS)–based X.25 routing feature, because the DNS server can search and provide all domains and addresses on a network.

With the DNS-based x.25 routing feature, it is easy to manage the X.121-to-IP addressing correlation and the mnemonic-to-X.121 addressing correlation. Instead of the router needing a route statement going to all destinations, all that is needed is a wildcard route statement that covers all addresses in the DNS.

# 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.

IP exchanges routing information using Routing Information Protocol (RIP), a dynamic distance-vector routing protocol. RIP is described in more detail in the following subsections.

## G.DMT

G.DMT full-rate ADSL is a technology that can expand the usable bandwidth of existing copper telephone lines, delivering high-speed data communications at rates of up to 10 Mbps. The technology brings full-motion video, efficient telecommuting, and high-speed data transmission to the home or business, all without interrupting normal telephone service.

American National Standards Institute (ANSI) has published an industry standard (known as T1.413) for full-rate ADSL in the United States. The International Telecommunication Union (ITU) has approved a nearly identical global industry standard for full-rate ADSL, known as G.992.1. The ANSI and ITU specifications call for operations rates of up to 8 Mbps downstream and up to 640 Kbps upstream when operating over telephone lines at a distance of up to 18,000 feet.

Standard-compliant full-rate ADSL uses a modulation technique known as discrete multitone, or DMT. DMT divides the upstream and downstream bands into a collection of smaller frequency ranges of approximately 4 kHz subchannel that carries a portion of the total data rate. By dividing the transmission bandwidth into a collection of subchannels, DMT is able to adapt to the distinct characteristics of each telephone line and maximize the data transmission rate. Telephone lines are best suited for transmission of the low frequencies associated with voice traffic (0–4 kHz). The high frequencies that are used for full-rate ADSL transmissions experience distortion and attenuation when sent over telephone lines- the higher the frequency, the more the attenuation. DMT effectively divides the data into a collection of smaller bandwidth transmissions, each of which occupies a smaller frequency range and is optimized to maximize the data throughput in that range. The ANSI and ITU standards have both established DMT as the standard modulation technique for full-rate ADSL.

## U-R2

U-R2 is a German Deutsche Telekom specification for ADSL over copper loops running ISDN in the base band (lower frequencies). It transmits and receives ADSL signals according to the ITU-T G.992.1 Annex B standard. It is a superset of the G.992.1 Annex B standard, allowing for greater cross-vendor interoperability.

# Routing Protocol Options

Routing protocols include the following:

- Routing Information Protocol (RIP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)

RIP and Enhanced IGRP protocols differ in several ways, as shown in Table 1-2.

*Table 1-2 RIP and EIGRP 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. |
| EIGRP | 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 plus incremental updates sent when the state of a destination changes. |

## RIP

RIP is an associated protocol for IP, and is widely used for routing Internet protocol traffic. 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, refer to the Cisco IOS 12.0(1)T documentation set. For information on accessing the documentation, see the "References to Cisco IOS Documentation Set" on page xxi.

## EIGRP

EIGRP 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 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 multi-protocol 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 originally emerged 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 illustrate how PAP works, imagine a network topology in which a remote office Cisco 827 router is connected to a corporate office Cisco 3600 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 illustrate how CHAP works, imagine a network topology in which a remote office Cisco 827 router is connected to a corporate office Cisco 3600 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 any time 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** Cisco recommends using CHAP because it is the more secure of the two protocols.

# TACACS+

Cisco 800 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 800 series routers support. The following network interface protocols are supported:

- Ethernet
- ATM
- ISDN

# 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 *Ethernet* is now often used to refer to all CSMA/CD LANs. Ethernet was designed to serve in networks with sporadic, occasionally heavy traffic requirements, and 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

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 traffic (UBR). Cisco 800 series routers also support AAL1 and 2 formats.

ATM encapsulation is the wrapping of data in a particular protocol header. The type of router you are connecting to determines the type of ATM PVC encapsulation types.

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 router's ATM subsystem 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 user to configure a backup modem line connection. The following can be used to bring up the dial backup feature in the Cisco IOS software:

- Backup Interface
- Floating Static Routers
- 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 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 and async lines and leased lines. The interfaces to such connections go up 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 alternate route. If this alternate 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 are able to 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 the 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, the 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 connected to the network temporarily 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, and configures the router to forward 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

**Note** When using NAT, DHCP relay cannot be used on the Cisco 800 series routers. The built-in DHCP server should be used instead.

# Cisco Easy VPN Client

Routers and other forms of broadband access provide high-performance connections to the Internet. However, many applications also require the security of Virtual Private Network (VPN) connections to perform a high level of authentication and to encrypt the data between two particular endpoints. Establishing a VPN connection between two routers can be complicated, and it typically requires tedious coordination between network administrators to configure the two routers’ VPN parameters.

The Cisco Easy VPN client feature eliminates much of this tedious work by implementing Cisco’s Unity Client protocol, which allows most VPN parameters to be defined at a VPN 3000 concentrator acting as an IPSec server.

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 800 series router. When the IPSec client then initiates the VPN tunnel connection, the IPSec server pushes the IPSec policies to the IPSec client and creates the corresponding VPN tunnel connection.

# VoIP

The Cisco 827-4V router is a voice-and-data-capable router that provides Voice-over-IP (VoIP) functionality and can carry voice traffic (such as telephone calls and faxes) over an IP network.

Cisco voice support is implemented using voice packet technology. There are two primary applications for VoIP:

- It provides a central-site telephony termination facility for VoIP traffic from multiple voice-equipped remote office facilities.
- It provides a PSTN gateway for Internet telephone traffic. VoIP used as a PSTN gateway leverages the standardized use of H.323-based Internet telephone client applications.

In VoIP, the digital signal processor (DSP) segments the voice signal into frames and stores them in voice packets. These voice packets are transported by using IP in compliance with H.323 signaling standards.

## H.323

H.323 is an International Telecommunication Union (ITU-T) standard that describes packet-based video, audio, and data conferencing. H.323 is an umbrella standard that describes the architecture of the conferencing system and refers to a set of other standards (H.245, H.225.0, and Q.931) to describe its actual protocol. Cisco H.323 Version 2 support upgrades Cisco IOS software to comply with the mandatory requirements and several of the optional features of the version 2 specification. This upgrade enhances the existing VoIP gateway and the Multimedia Conference Manager (gatekeeper and proxy). A *gateway* allows H.323 terminals to communicate with non-H.323 terminals by converting protocols, and it is an endpoint on the LAN that provides real-time, two-way communications between H.323 terminals on the LAN and other ITU-T terminals in the WAN or to another H.323 gateway.

The *gatekeeper* maintains a registry of devices in the multimedia network. The devices register with the gatekeeper at startup and request admission to a call from the gatekeeper. The gatekeeper is an H.323 entity on the LAN that provides address translation and control access to the LAN for H.323 terminals and gateways. The gatekeeper may provide other services to the H.323 terminals and gateways, such as bandwidth management and locating gateways.

## Voice Dial Peers

Dial peers enable outgoing calls from a particular telephony device. All of the voice technologies use dial peers to define the characteristics associated with a *call leg*.

A call leg is a discrete segment of a call connection that lies between two points in the connection. It is important to remember that these terms are defined from the *router* perspective. An inbound call leg means that an incoming call comes *to* the router. An outbound call leg means that an outgoing call is placed *from* the router. Dial peers are used for both inbound and outbound call legs.

For inbound call legs, a dial peer might be associated with the calling number or the voice-port number. Outbound call legs always have a dial peer associated with them. The destination pattern is used to identify the outbound dial peer. The call is associated with the outbound dial peer at setup time.

There are two kinds of dial peers that need to be configured for each voice implementation:

- POTS—(also known as “plain old telephone service” or “basic telephone service”) dial peer associates a physical voice port with a local telephone device. The key commands in your configuration are the **port** and **destination-pattern** commands. The **destination-pattern** command defines the telephone number associated with the POTS dial peer. The **port** command associates the POTS dial peer with a specific logical dial interface, normally the voice port connecting your router to the local POTS network.
- VoIP—dial peer associates a telephone number with an IP address. The key commands in your configuration are the **destination-pattern** and **session target** commands.The **destination-pattern** command defines the telephone number associated with the VoIP dial peer. The **session target** command specifies a destination IP address for the VoIP dial peer. In addition, you can use VoIP dial peers to define characteristics such as IP precedence, additional QoS parameters, and codec.

# 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 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, or 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 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 queueing 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 characterize 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.

# Committed Access Rate

Committed access rate (CAR) can be used to limit bandwidth or transmission rates based on traffic sources and destinations and to specify policies for handling traffic that breaches the specified bandwidth allocations. CAR provides configurable actions, such as transmit, drop, set precedence, or set QoS group, when traffic conforms to or exceeds the rate limit.

The CAR feature performs the following functions:

- Limits the input or output transmission rate on an interface or subinterface, based on a flexible set of criteria.
- Classifies packets by setting the IP Precedence or QoS group, which is a class identifier that is internal to the router.

To enable CAR, enter the **rate-limit** command while in ATM interface configuration mode.

## Rate Limitation

The rate limitation feature of CAR provides the network operator with the means to define Layer 3 aggregate or granular access, or egress bandwidth rate limits, and to specify traffic handling policies when the traffic either conforms to or exceeds the specified rate limits. Aggregate access or egress matches all packets on an interface or subinterface. Granular access or egress matches a particular type of traffic based on precedence. You can designate CAR rate limitation policies based on physical port, packet classification, IP address, MAC address, application flow, and other criteria specifiable by access lists or extended access lists. CAR rate limits may be implemented either on input or output interfaces or subinterfaces including Frame Relay and ATM subinterfaces.

An example of the use of the rate-limiting capability of CAR is application-based rates limiting HTTP World Wide Web traffic to 50 percent of link bandwidth, which ensures capacity for non-Web traffic including mission-critical applications.

## Marking of IP Precedence

Extended access list classification can be used to set precedence that might be needed for features like class-based traffic shaping and CAR. This allows considerable flexibility for precedence assignment, including assignment by application or user, or 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 CBWFQ), with no changes to existing applications or complicated network requirements.

## Weighted Fair Queuing

Weighted fair queuing (WFQ) enables slow-speed links, such as serial links, to provide fair treatment for all types of traffic. WFQ classifies the traffic into different flows (also known as *conversations*) based on Layer 3 and Layer 4 information, such as IP addresses and TCP ports. WFQ performs this classification without requiring you to define access lists. This means that low-bandwidth traffic effectively has priority over high-bandwidth traffic because high-bandwidth traffic shares the transmission media in proportion to its assigned weight. WFQ is now available on IP Base and IP Firewall Cisco IOS images.

## Weighted Random Early Detection

Random early detection (RED) is a congestion-avoidance mechanism that takes advantage of TCP's congestion control mechanism. By randomly dropping packets prior to periods of high congestion, RED tells the packet source to decrease its transmission rate. Assuming that the packet source is using TCP, it will decrease its transmission rate until all the packets reach their destination, indicating that the congestion is cleared.

Weighted RED (WRED), the Cisco implementation of RED, generally drops packets selectively, based on IP precedence. Packets with a higher IP precedence are less likely to be dropped than packets with a lower precedence. Thus, higher priority traffic is delivered with a higher probability than lower priority traffic. It can selectively discard lower priority traffic when the interface begins to get congested and provide differentiated performance characteristics for different classes of service. WRED is also RSVP-aware.

## ATM Traffic Policing

The traffic policing feature performs the following functions:

- Limits the input or output transmission rate of a class of traffic, based on user-defined criteria
- Marks packets by setting the IP Precedence value, the QoS group, or the differentiated service code point (DSCP) value

## 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.

# Configuring Basic Networks

This chapter describes three networks that network administrators in small independent offices or that telecommuters can set up. You can familiarize yourself with the three networks, determining which one is best suited for your situation.

Following are the three basic network types:

- Private IP network to Internet
- Public IP network to Internet
- Remote office network to corporate office network using IP

The following sections contain information about preparing for the configurations and the steps to configure each of the three basic networks.

## Before Configuring Basic Networks

Before configuring the three basic networks, you must do the following:

**Step 1** If using ISDN, order an ISDN line from your telephone service provider. For complete information on ordering your ISDN line, see Appendix D, "Provisioning an ISDN Line."

**Step 2** While ordering your ISDN line, gather the following information from your telephone service provider:

- ISDN switch type.
- Service profile identifiers (SPIDs). Only telephone service providers in North America assign SPIDs. SPIDs identify the ISDN B channels. The SPID format is generally an ISDN telephone number with additional numbers at the end; for example, 40855522220101. Depending on the switch that supports your ISDN line, your ISDN line could be assigned zero, one, or two SPIDs.
- ISDN local directory numbers (LDNs), which are the local ISDN telephone numbers of your router. Examples are 4085552222 or 5553333.

**Note** The format of the LDN varies from region to region, depending on the telephone service provider. In some regions, you need to add the area code to the telephone number. Find out from your local telephone service provider whether or not you need to specify an area code for the LDN.

**Step 3** If setting up an Internet connection, gather the following information from your Internet service provider (ISP):

- Point-to-Point Protocol (PPP) client name that the ISP assigns as your login name.
- PPP authentication type: Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP).
- PPP password to access your ISP account.
- IP address information: the IP address and subnet mask of the ISP ISDN interface. Also, if configuring a public IP network, you must gather the registered IP addresses and subnet masks to be used on your router LAN and WAN interfaces.
- ISP telephone number.

**Step 4** If setting up a connection to a corporate network, you and the network administrator of the corporate network must decide on or generate the following information for the WAN interfaces of the routers so you can both use this information:

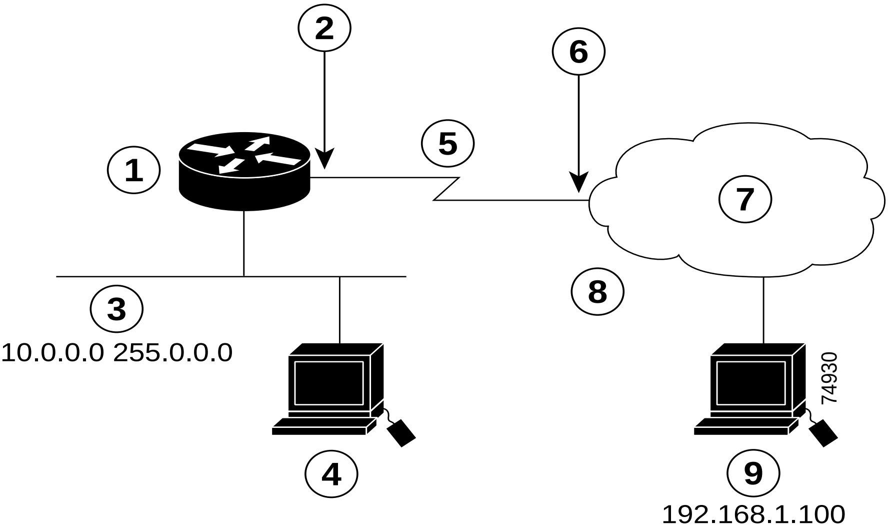
- PPP authentication type: CHAP or PAP.
- PPP client name to access the router.
- PPP password to access the router.
- Telephone number assigned to the telephone interface of your router.

**Step 5** If setting up IP routing, obtain the addressing scheme information for your IP network.

# Connecting a Private IP Network to the Internet

In the network example shown in Figure 2-1 and Table 2-1, the Cisco 800 series router connects a private IP network to an ISP.

*Figure 2-1 Connecting Private IP Network to Internet*



| Callout Number | Description |
|---|---|
| **1** | DHCP server at Site 1 |
| **2** | National ISDN-1 switch type, with B1 SPID 40855511110101 and B2 SPID 40855522220101 |
| **3** | Private IP network |
| **4** | DHCP client |
| **5** | PPP link |
| **6** | ISDN phone number, 4085551111 |
| **7** | Internet service provider |
| **8** | CHAP or PAP |
| **9** | Domain Name System (DNS) server |

## Features Used

This network uses the following features on the LAN:

- IP routing
- Dynamic Host Configuration Protocol (DHCP) server (optional)

When your router is acting as a DHCP server, workstations configured as DHCP clients are automatically assigned an IP address and subnet mask.

This network uses the following features on the WAN:

- IP routing
- PPP
- Network Address Translation (NAT) overload
- Internet Protocol Control Protocol (IPCP)
- CHAP or PAP over PPP
- Dial-on-demand routing (DDR)
- Static routes

With NAT overload configured, the router uses one address for multiple hosts. With IPCP configured, your router automatically negotiates its IP address from the router it is attempting to connect to.

You can use either CHAP or PAP as the PPP authentication protocol. Cisco recommends using CHAP, because it is the more secure of the two protocols.

In addition, the ISDN line is activated only when needed (DDR), using one route that has been manually configured (static route). DDR using static routes suits small networking environments that do not have complex routing topologies.

# Configuration

To configure the features for this network example, perform the following steps on the PC, starting in global configuration mode.

**Step 1** Specify a name for the router. For example, specify *SanJose* as the router name:

```
router(config)# hostname SanJose
```

**Step 2** Specify an encrypted password containing from 1 to 25 uppercase or lowercase alphanumeric characters. Spaces are also valid password characters. Leading spaces are ignored; trailing spaces are recognized. For example, specify *abra cadabra* as the password:

```
SanJose(config)# enable secret abra cadabra
```

**Step 3** Configure the router to recognize the zero subnet range as a valid range of addresses:

```
SanJose(config)# ip subnet-zero
```

**Step 4** Disable the router from translating unfamiliar words entered during a console session into IP addresses:

```
SanJose(config)# no ip domain-lookup
```

**Step 5** Optional. Configure your router as a DHCP server. Define the DHCP relay pool name. For example:

```
router(config)# ip dhcp pool DHCPpoolLAN_0
```

**a.** Set the DHCP pool of addresses. For example:

```
router(dhcp-config)# network 10.0.0.0 255.255.255.0
```

**b.** Set the IP addresses of the DNS servers. For example:

```
router(dhcp-config)# dns-server 192.168.1.100
```

**c.** Set the NetBIOS servers. For example:

```
router(dhcp-config)# netbios-name-server
10.1.1.2 10.1.1.3
```

**d.** Set the Ethernet 0 IP address as the default gateway. For example:

```
router(dhcp-config)# default-router 10.0.0.1
```

**e.** Exit to global configuration mode:

```
router(dhcp-config)# exit
```

**Step 6** Configure the LAN interface by performing the following steps:

**a.** Specify parameters for the LAN interface:

```
SanJose(config)# interface ethernet0
```

**b.** Set the IP address and subnet mask for the LAN interface. For example:

```
SanJose(config-if)# ip address 10.0.0.1 255.0.0.0
```

**c.** Activate the LAN interface:

```
SanJose(config-if)# no shutdown
```

**Step 7** Enable NAT on your LAN. The inside network address is not directly routed to the Internet, but is subject to translation to a routable address outside the LAN. For example:

```
SanJose(config-if)# ip nat inside
```

**Step 8** Configure the WAN interface by performing the following steps:

**a.** Change to global configuration mode:

```
SanJose(config-if)# exit
SanJose(config)#
```

**b.** Specify parameters for the WAN interface:

```
SanJose(config)# interface bri0
```

**c.** Enable PPP:

```
SanJose(config-if)# encapsulation ppp
```

**d.** Enable multilink PPP:

```
SanJose(config-if)# ppp multilink
```

**e.** Enable the translation of the inside network to a valid Internet address:

```
SanJose(config-if)# ip nat outside
```

**f.** Create a dialer rotary group, specifying a number between 0 and 255. Dialer rotary groups are useful in environments that require multiple calling destinations. For example:

```
SanJose(config-if)# dialer rotary-group 0
```

**g.** North America only. Associate the ISDN local directory numbers (LDNs) provided by your telephone service provider with the first and second SPIDs. You can specify the SPID number, or you can have it automatically detected by entering a **0**.

In the following example, the SPID number is represented by a **0,** so that it will be automatically detected. The primary LDN is followed by the secondary LDN for each SPID.

```
SanJose(config-if)# isdn spid1 0 4085551111 4085552222
SanJose(config-if)# isdn spid2 0 4085553333 4085554444
```

**Note** Find out from your telephone service provider whether you need to specify an area code for the LDN.

**h.** North America only. If you had manually entered the SPID number, enable the BRI0 interface.

```
SanJose(config-if)# no shutdown
```

**i.** North America only. If you configured the SPID to be automatically detected, enable the automatic detection of ISDN SPID numbers and switch type:

```
SanJose(config-if)# isdn autodetect
```

**j.** Outside of North America only. Specify the ISDN switch type. To get a listing of supported switches, enter the **isdn switch-type ?** command.

The following example specifies the NET3 switch type:

```
router(config-if)# isdn switch-type basic-net3
```

k. Disable the Cisco Discovery Protocol (CDP):

```
SanJose(config-if)# no cdp enable
```

**Step 9** Follow these steps to specify characteristics of the dialer rotary group that were created in the previous step:

a. Change to global configuration mode:

```
SanJose(config-if)# exit
SanJose(config)#
```

b. Create a dialer interface, specifying a number between 0 to 255 to represent your dialer rotary group. For example:

```
SanJose(config)# interface dialer 0
SanJose(config-if)#
```

c. Specify that the IP address for this interface is obtained by using IPCP:

```
SanJose(config-if)# ip address negotiated
```

d. Enable PPP as the encapsulation type:

```
SanJose(config-if)# encapsulation ppp
```

e. Enable DDR:

```
SanJose(config-if)# dialer in-band
```

f. Specify the amount of time in number of seconds that the line can be idle before it is disconnected:

```
SanJose(config-if)# dialer idle-timeout 300
```

g. Specify the telephone number of the interface to be called if you are calling a single site. For example:

```
SanJose(config-if)# dialer string 14085553333
```

h. Set the maximum number of packets to be held in the outgoing queue to 10. If an ISDN connection does not exist yet, the hold queue holds up to 10 packets before dropping them. For example:

```
SanJose(config-if)# dialer hold-queue 10
```

**i.** Define the load level that must be exceeded on the first ISDN B channel before the second B channel is brought up. The *load-threshold* variable represents a utilization percentage and is a number between 1 and 255, where 255 equals 100 percent. For example:

```
SanJose(config-if)# dialer load-threshold 10 outbound
```

**Note** Enter **outbound** to calculate the load using outbound data only, **inbound** to calculate the load using inbound data only, and **either** to set the maximum calculated load as the larger of the outbound and inbound loads.

**j.** Assign this interface to dialer access group 1:

```
SanJose(config-if)# dialer-group 1
```

**k.** Configure CHAP, then specify a CHAP host name and password. To configure PAP, skip this step and go to the next step.

This command enables CHAP and specifies authentication on incoming calls only. Unidirectional authentication is used because non-Cisco routers that do not support bidirectional authentication are potentially in use at the ISP. In these cases, when the SanJose router calls the ISP, SanJose does not authenticate. However, the ISP authenticates SanJose before allowing the connection.

```
SanJose(config-if)# ppp authentication chap callin
router(config-if)# ppp chap hostname SanJose
router(config-if)# ppp chap password gocisco1
```

**l.** Configure PAP. To configure CHAP, skip this step and follow the previous step.

The following command enables PAP and specifies authentication on incoming calls only. Unidirectional authentication is used because routers that do not support bidirectional authentication are potentially in use at the ISP. In these cases, when the SanJose router calls the ISP, SanJose does not authenticate. However, the ISP authenticates SanJose before allowing the connection.

```
SanJose(config-if)# ppp authentication pap callin
```

**m.** Enable remote PAP support for an interface. The username and password are sent in the PAP authentication request packet. The password must contain from 1 to 25 upper- and lowercase alphanumeric characters; it cannot contain spaces nor underscores.

```
SanJose(config-if)# ppp pap sent-username SanJose
password gocisco
```

**n.** Enable multilink PPP:

```
SanJose(config-if)# ppp multilink
```

**Step 10** Follow these steps to configure how the IP routing protocol learns routes:

**a.** Change to global configuration mode:

```
SanJose(config-if)# exit
SanJose(config)#
```

**b.** Set up all IP addresses to be treated as classless:

```
SanJose(config)# ip classless
```

**c.** Enable IP routing and set up a static route. Typically, the ISP does not provide IP addresses and subnet masks of their networks, but they do provide the IP address of the ISDN router interface to which your router is connected.

The following example specifies that you need to use dialer 0 on your router to reach the ISP router. Dialer 0 had been previously configured using the **interface dialer** command.

```
SanJose(config)# ip routing
SanJose(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1
SanJOse(config)# ip route 192.168.1.1 255.255.255.255 dialer0
```

**Step 11** Specify that dialer-list 1 permits dialing by the IP routing protocol:

```
SanJose(config)# dialer-list 1 protocol ip permit
```

**Step 12** Perform this step only if ISDN calls at 64 kbps are not supported. Specify characteristics of the outgoing calls from an ISDN interface by using the following steps:

**a.** Define a class of shared configuration parameters for outgoing calls from an ISDN interface:

```
SanJose(config)# map-class dialer 56k
```

The unique identifier that identifies the class is 56k.

**b.** Specify 56 kbps as the B channel speed:

```
SanJose(config-map-class)# dialer isdn speed 56
```

**Step 13** If you have a Cisco 800 series router that is connected to a telephone, fax machine, or modem, configure the telephone interfaces by performing the following steps:

**a.** Change to global configuration mode:

```
SanJose(config-map-class)# exit
SanJose(config)#
```

**b.** Specify the country where your router is located:

```
SanJose(config)# pots country us
```

Enter the **pots country ?** command to get a list of supported countries and codes.

This command determines the physical characteristics of the telephone interfaces. By specifying a country, you are configuring your telephone to use country-specific default settings for each of the physical characteristics.

**c.** Create dial peers to determine how incoming calls are routed to the telephone ports. In the following example, the dial-peer tag is 1, the ISDN local directory number LDN is 5551111, the telephone port is 1, and call waiting is disabled:

```
SanJose(config)# dial-peer voice 1 pots
SanJose(config-dial-peer)# destination-pattern 5551111
SanJose(config-dial-peer)# port 1
SanJose(config-dial-peer)# no call-waiting
SanJose(config-dial-peer)# exit
SanJose(config)#
```

**Note** Enter a number between 1 and 6 for the dial-peer *tag* variable.

Find out from your telephone service provider whether or not you need to specify an area code for the LDN.

**d.** Specify parameters for the WAN interface:

```
SanJose(config)# interface bri0
```

**e.** Specify that incoming voice calls shall be forwarded to the devices connected to the telephone ports:

```
SanJose(config-if)# isdn incoming-voice modem
```

**Step 14** Exit the interface configuration mode.

```
SanJose(config-if)# exit
SanJose#(config)#
```

**Step 15** In global configuration mode, set global NAT commands. In the following example, all inside network addresses assigned to interface BRI0 are configured for translation, and the access list that contains the inside network addresses is defined.

```
SanJose(config)# ip nat inside source list 1 interface bri0
overload
SanJose(config)# access-list 1 permit 10.0.0.0 255.0.0.0
```

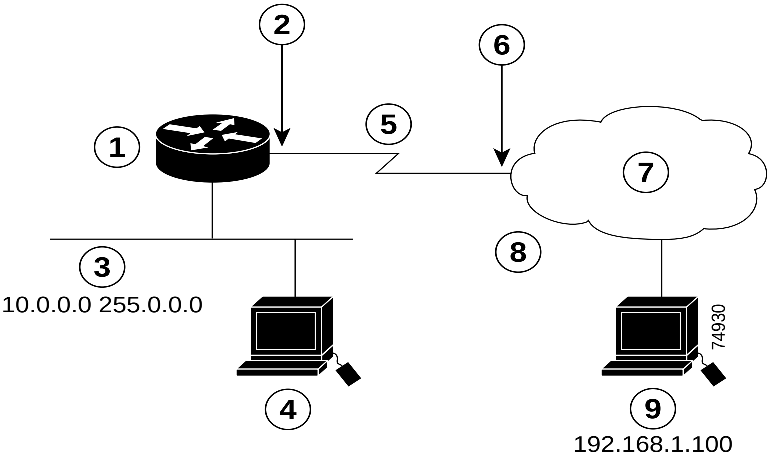
**Step 16** Change to user mode and save your configuration:

```
SanJose(config)# exit
SanJose# copy running-config startup-config
```

# Connecting a Public IP Network to the Internet

In the network example shown in Figure 2-2 and Table 2-2, the Cisco 800 series router connects a public IP network to an ISP. The ISP has assigned a range of registered (public) IP addresses for the LAN devices that require Internet access.

*Figure 2-2 Connecting a Public IP Network to the Internet*



| Callout Number | Description |
|---|---|
| **1** | DHCP server at Site 1 |
| **2** | National ISDN-1 switch type, with B1 SPID 40855511110101 and B2 SPID 40855522220101 |
| **3** | Private IP network |
| **4** | DHCP client |
| **5** | PPP link |
| **6** | ISDN phone number, 4085551111 |
| **7** | Internet service provider |
| **8** | CHAP or PAP |
| **9** | Domain Name System (DNS) server |

# Features Used

This network uses the following features on the LAN:

- IP routing
- DHCP server (optional)

When your router is acting as a DHCP server, workstations configured as DHCP clients are automatically assigned IP addresses and subnet masks.

This network uses the following features on the WAN:

- IP routing
- PPP
- IPCP (optional)
- CHAP or PAP over PPP
- DDR
- Static routes

If the ISP does not assign an IP address and subnet mask for your WAN interface, you can use IPCP to automatically negotiate its IP address from the router to which it is attempting to connect.

You can use either CHAP or PAP as the PPP authentication protocol. Cisco recommends using CHAP because it is the more secure of the two protocols.

In addition, the ISDN line is activated only when needed (DDR), using one route that has been manually configured (static route). DDR using static routes suits small networking environments that do not have complex routing topologies.

# Configuration

To configure the features for this network example, perform the following steps on the PC, starting in the global configuration mode.

**Step 1** Specify a name for the router. For example, specify *SanJose* as the router name:

```
router(config)# hostname SanJose
```

**Step 2** Specify an encrypted password containing from 1 to 25 uppercase or lowercase alphanumeric characters. Spaces are valid password characters. Leading spaces are ignored but trailing spaces are recognized. For example:

```
SanJose(config)# enable secret abra cadabra
```

**Step 3** Configure the router to recognize the zero subnet range as a valid range of addresses:

```
SanJose(config)# ip subnet-zero
```

**Step 4** Disable the router from translating unfamiliar words entered during a console session into IP addresses:

```
SanJose(config)# no ip domain-lookup
```

**Step 5** Optional. Configure your router as a DHCP server.

**a.** Define the DHCP relay pool name. For example:

```
router(config)# ip dhcp pool DHCPpoolLAN_0
```

**b.** Set the DHCP pool of addresses. For example:

```
router(dhcp-config)# network 10.0.0.0 255.255.255.0
```

**c.** Set the IP addresses of the DNS servers. For example:

```
router(dhcp-config)# dns-server 192.168.1.100
```

**d.** Set the NetBIOS servers. For example:

```
router(dhcp-config)# netbios-name-server
10.1.1.2 10.1.1.3
```

**e.** Set the Ethernet 0 IP address as the default gateway. For example:

```
router(dhcp-config)# default-router 10.1.1.1
```

**f.** Exit to global configuration mode.

```
router(dhcp-config)# exit
```

**Step 6** Configure the LAN interface by performing the following steps:

**a.** Specify parameters for the LAN interface:

```
SanJose(config)# interface ethernet0
```

**b.** Set an IP address and subnet mask for the LAN interface. For example, set the IP address and subnet mask to 10.1.1.1 and 255.0.0.0, respectively:

```
SanJose(config-if)# ip address 10.1.1.1 255.0.0.0
```

**Step 7** Configure the WAN interface by performing the following steps:

**a.** Change to global configuration mode:

```
SanJose(config-if)# exit
SanJose(config)#
```

**b.** Specify parameters for the WAN interface:

```
SanJose(config)# interface bri0
SanJose(config-if)#
```

**c.** Enable PPP:

```
SanJose(config-if)# encapsulation ppp
```

**d.** Enable multilink PPP:

```
SanJose(config-if)# ppp multilink
```

**e.** Create a dialer rotary group, specifying a number between 0 and 255. Dialer rotary groups are useful in environments that require multiple calling destinations. For example:

```
SanJose(config-if)# dialer rotary-group 0
```

**f.** North America only. Associate the ISDN local directory numbers (LDNs) provided by your telephone service provider to the first and second SPIDs. You can specify the SPID number or you can have it automatically detected by entering a **0**.

In the following example, the SPID number is represented by a **0** so that it will be automatically detected. The primary LDN is followed by the secondary LDN for each SPID.

```
SanJose(config-if)# isdn spid1 0 4085551111 4085552222
SanJose(config-if)# isdn spid2 0 4085553333 4085554444
```

**Note** Find out from your telephone service provider whether or not you need to specify an area code for the LDN.

g. North America only. If you had manually entered the SPID number, enable the BRI0 interface.

```
SanJose(config-if)# no shutdown
```

h. North America only. If you had specified the automatic detection of SPID numbers, enable the automatic detection of ISDN SPID numbers and switch type:

```
SanJose(config-if)# isdn autodetect
```

i. Outside of North America only. Specify the ISDN switch type. To see a listing of supported switches, enter the **isdn switch-type ?** command.

The following example specifies the NET3 switch:

```
SanJose(config-if)# isdn switch-type basic-net3
```

j. Disable Cisco Discovery Protocol (CDP).

```
SanJose(config-if)# no cdp enable
```

**Step 8** Follow these steps to specify characteristics of the dialer rotary group that you created earlier:

a. Change to global configuration mode:

```
SanJose(config-if)# exit
SanJose(config)#
```

b. Create a dialer rotary group leader and specify a number between 0 to 255 to represent your dialer rotary group. For example:

```
SanJose(config)# interface dialer 0
```

c. Set the IP address and subnet mask for the WAN interface provided by the ISP. For example:

```
SanJose(config-if)# ip address 192.168.1.2 255.255.255.0
```

d. Optional. If the ISP did not provide an IP address and subnet mask for the WAN interface, set up IPCP to obtain them from the router to which it is connecting:

```
SanJose(config-if)# ip address negotiated
```

e. Enable PPP:

```
SanJose(config-if)# encapsulation ppp
```

**f.** Enable DDR:

```
SanJose(config-if)# dialer in-band
```

**g.** Specify the amount of time (in seconds) that the line can be idle before it is disconnected. For example:

```
SanJose(config-if)# dialer idle-timeout 300
```

**h.** Specify a telephone number of the interface to be called if you are calling a single site. Enter the number 1 plus the telephone number if it is a long distance call. For example:

```
SanJose(config-if)# dialer string 14085553333
```

**i.** Set the number of packets to be held in the outgoing queue to 10. If an ISDN connection does not exist yet, the hold-queue holds up to 10 packets before dropping them. For example:

```
SanJose(config-if)# dialer hold-queue 10
```

**j.** Define the load level that must be exceeded on the first ISDN B channel before the second B channel is brought up. The *load-threshold* variable represents a utilization percentage and is a number between 1 and 255, where 255 equals 100 percent.

```
SanJose(config-if)# dialer load-threshold 10 outbound
```

**Note** Enter **outbound** to calculate the load using outbound data only, **inbound** to calculate the load using inbound data only, and **either** to set the maximum calculated load as the larger of the outbound and inbound loads.

**k.** Assign this interface to dialer access group 1:

```
SanJose(config-if)# dialer-group 1
```

**l.** Enable CHAP and configure the CHAP hostname and password. To configure PAP, skip this step, and go on to the next step.

This command enables CHAP and specifies authentication on incoming calls only. Unidirectional authentication is used because non-Cisco routers that do not support bidirectional authentication are potentially in use at the ISP. In these cases, when SanJose calls the ISP, SanJose does not authenticate. However, the ISP authenticates SanJose before allowing the connection. For example:

```
SanJose(config-if)# ppp authentication chap callin
SanJose(config-if)# ppp chap hostname SanJose
SanJose(config-if)# ppp chap password gocisco1
```

**m.** Configure PAP. To configure CHAP, skip this step, and follow the previous step.

```
SanJose(config-if)# ppp authentication pap callin
```

This command enables PAP and specifies authentication on incoming calls only. Unidirectional authentication is used because non-Cisco routers that do not support bidirectional authentication are potentially in use at the ISP. In these cases, when the SanJose router calls the ISP, the SanJose router does not authenticate the ISP router. However, the ISP authenticates the SanJose router before allowing the connection.

**n.** Enable remote PAP support for an interface. In the following example, the username and password (*SanJose* and *gocisco1*, respectively) are sent in the PAP authentication request packet. The password must contain from 1 to 25 uppercase and lowercase alphanumeric characters and cannot contain spaces or underscores.

```
SanJose(config-if)# ppp pap sent-username SanJose
password gocisco1
```

**o.** Enable multilink PPP:

```
SanJose(config-if)# ppp multilink
```

**Step 9** Follow these steps to configure how the IP routing protocol learns the routes:

**a.** Change to global configuration mode:

```
SanJose(config-if)# exit
SanJose(config)#
```

**b.** Configure all IP addresses to be treated as classless:

```
SanJose(config)# ip classless
```

c. Set up static routes by entering the destination network, destination subnet mask, and the next hop address. In the following example, the IP address of the ISP router ISDN interface is 192.168.1.1. Typically, the ISPs do not provide IP addresses and subnet masks of their networks, but they do provide the IP addresses of the ISDN interfaces to which your router connects.

The following example specifies 0.0.0.0 and 0.0.0.0 as the IP address and subnet mask of the ISP network, because you would not know these addresses.

```
SanJose(config)# ip route 0.0.0.0 0.0.0.0 dialer0
```

**Step 10** Specify that dialer-list 1 permits dialing by the IP routing protocol:

```
SanJose(config)# dialer-list 1 protocol ip permit
```

**Step 11** Perform this step only if ISDN calls at 64 kbps are not supported. Follow these steps to specify the characteristics of outgoing calls from an ISDN interface. The unique identifier for the class is 56k.

a. Define a class of shared configuration parameters for outgoing calls from an ISDN interface:

```
SanJose(config)# interface dialer 0
SanJose(config-if)# dialer string 5551212 class 56k
SanJose(config-if)# exit
SanJose(config)# map-class dialer 56k
```

b. Specify 56 kbps as the B channel speed:

```
SanJose(config-map-class)# dialer isdn speed 56
```

c. Change to global configuration mode:

```
SanJose(config-map-class)# exit
SanJose(config)#
```

**Step 12** If you have a Cisco 800 series router that is connected to a telephone, fax machine, or modem, configure the telephone interfaces by performing the following steps:

a. Specify the country where your router is located. For example:

```
SanJose(config)# pots country us
```

This command determines the physical characteristics of the telephone interfaces. By specifying a country, you are configuring your telephone to use country-specific default settings for each of the physical characteristics. To get a list of supported countries and the code, enter the **pots country ?** command.

**b.** Create dial peers to determine how incoming calls are routed to the telephone ports. In the following example, the dial-peer tag is 1, the ISDN local directory number (LDN) is 5551111, the telephone port is 1, and call waiting is disabled:

```
SanJose(config)# dial-peer voice 1 pots
SanJose(config-dial-peer)# destination-pattern 5551111
SanJose(config-dial-peer)# port 1
SanJose(config-dial-peer)# no call-waiting
SanJose(config-dial-peer)# exit
```

**Note** Enter a number between 1 and 6 for the dial-peer *tag* variable.

Find out from your telephone service provider whether or not you need to specify an area code for the LDN.

**c.** Specify parameters for the WAN interface:

```
SanJose(config)# interface bri0
```

**d.** Specify that incoming voice calls are forwarded to the devices connected to the telephone ports:

```
SanJose(config-if)# isdn incoming-voice modem
```

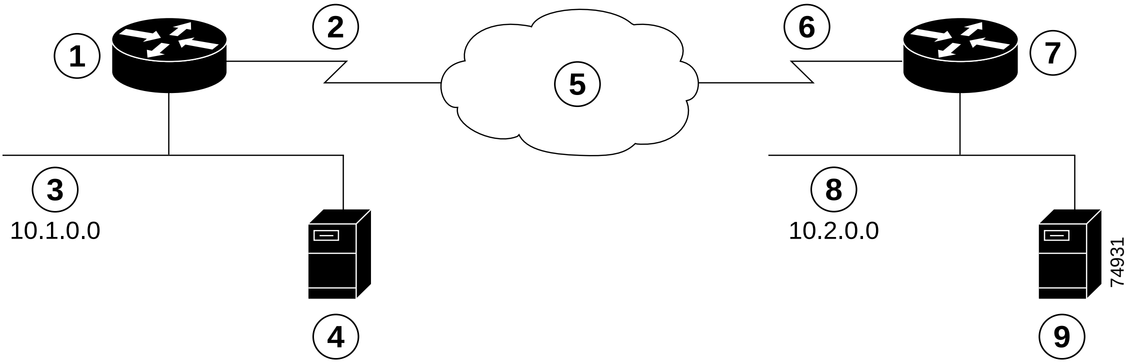
**e.** Change to user mode and save your configuration:

```
SanJose(config-if)# end
SanJose# copy running-config startup-config
```

# Connecting a Remote Office to a Corporate Office

In the network example shown in Figure 2-3 and Table 2-3, the Cisco 800 series router and another router, such as a Cisco 3600 router, connect the networks of a remote office and a corporate office by using a dial-on-demand ISDN line. The routes between the two routers are static IP routes that you configure.

*Figure 2-3 Remote Office to Corporate Office*



| Callout Number | Description |
|---|---|
| **1** | Site 1 |
| **2** | National ISDN-1 switch type, with B1 SPID 40855511110101 and B2 SPID 40855522220101 |
| **3** | IP network at Site 1 |
| **4** | File server on Site 1 network |
| **5** | PPP link |
| **6** | ISDN phone number, 4085551111 |
| **7** | Internet service provider |
| **8** | CHAP or PAP |
| **9** | Domain Name System (DNS) server |

| | | | |
|---|---|---|---|
| **1** | Site 1 | **6** | 5ESS custom multipoint switch type, with B1 SPID 0155533330101 / B2 SPID 0155544440101 |
| **2** | | **7** | Site 2 |
| **3** | | **8** | IP network at Site 2 |
| **4** | | **9** | File server at Site 2 |
| **5** | ISDN network connection | | |

## Features Used

This network uses the following features on the LAN:

- IP routing (Cisco recommends this for management purposes, such as Telnet)
- DHCP server (optional)

When your router is acting as a DHCP server, workstations configured as DHCP clients are automatically assigned an IP address and subnet mask.

This network uses the following features on the WAN:

- IP routing
- PPP
- IPCP
- CHAP or PAP over PPP
- DDR
- Static routes

With IPCP configured, your router automatically negotiates its IP address from the router it is attempting to connect.

You can use either CHAP or PAP as the PPP authentication protocol. Cisco recommends using CHAP because it is the more secure of the two protocols.

Because DDR is configured, the ISDN line is activated only when needed using one route that has been manually configured (static route). Because a static route is configured, the routers do not need to exchange routing updates. As a result, the ISDN line is activated only when traffic demands.

# Cisco 800 Series Router Configuration

To configure the features for this network example, perform the following steps on the PC, starting in the global configuration prompt.

**Step 1** Specify a name for the router. For example:

```
router(config)# hostname SanJose
```

**Step 2** Specify an encrypted password. For example:

```
SanJose(config)# enable secret password
```

**Step 3** Specify the username of any client that will potentially dial into your router and the password that your router and the client will share. Specify the username and password of the central office router (the central office network administrator should provide this information). For example:

```
SanJose(config)# username LosAngeles password gocisco1
```

**Step 4** Optional. Configure your router as a DHCP server:

**a.** Define the DHCP relay pool name. For example:

```
router(config)# ip dhcp pool DHCPpoolLAN_0
```

**b.** Set the DHCP pool of addresses. For example:

```
router(dhcp-config)# network 10.1.0.0 255.255.0.0
```

**c.** Set the IP addresses of the DNS servers. For example:

```
router(dhcp-config)# dns-server 192.168.1.0 255.255.255.0
```

**d.** Set the Ethernet 0 IP address as the default gateway. For example:

```
router(dhcp-config)# default-router 10.1.0.1
```

**Step 5** Configure the WAN interface by performing the following steps:

**a.** Change to global configuration mode:

```
SanJose(dhcp-config)# exit
SanJose(config)#
```

**b.** Specify parameters for the WAN interface:

```
SanJose(config)# interface bri0
SanJose(config-if)#
```

c. Enable PPP:

```
SanJose(config-if)# encapsulation ppp
```

d. Enable multilink PPP:

```
SanJose(config-if)# ppp multilink
```

e. Create a dialer rotary group, specifying a number between 0 and 255. Dialer rotary groups are useful in environments that require multiple calling destinations. For example:

```
SanJose(config-if)# dialer rotary-group 0
```

f. North America only. Associate the ISDN local directory numbers (LDNs) provided by your telephone service provider to the first and second SPIDs. You can specify the SPID number or you can have it automatically detected by entering a **0**.

In the following example, the SPID number is represented by a **0** so that it would be automatically detected. The primary LDN is followed by the secondary LDN for each SPID.

```
SanJose(config-if)# isdn spid1 0 4085551111 4085552222
SanJose(config-if)# isdn spid2 0 4085553333 4085554444
```

**Note** Find out from your telephone service provider whether you need to specify an area code for the LDN.

g. North America only. If you had entered the SPID number, enable the BRI0 interface.

```
SanJose(config-if)# no shutdown
```

h. North America only. If you configured the SPID to be automatically detected, enable the automatic detection of ISDN SPID numbers and switch type:

```
SanJose(config-if)# isdn autodetect
```

i. Outside of North America only. Specify the ISDN switch type. To see a listing of supported switches, enter the **isdn switch-type ?** command.

The following example specifies the NET3 switch:

```
SanJose(config-if)# isdn switch-type basic-net3
```

j. Disable CDP.

```
SanJose(config-if)# no cdp enable
```

**Step 6** Specify the characteristics of the dialer rotary group that you created earlier by performing the following steps:

a. Change to global configuration mode:

```
SanJose(config-if)# exit
SanJose(config)#
```

b. Create a virtual interface by specifying a number between 0 to 255 to represent your dialer rotary group.

```
SanJose(config)# interface dialer 0
```

c. Enable PPP:

```
SanJose(config-if)# encapsulation ppp
```

d. Enable DDR:

```
SanJose(config-if)# dialer in-band
```

e. Specify the amount of time (in seconds) that the line can be idle before it is disconnected. For example:

```
SanJose(config-if)# dialer idle-timeout 300
```

f. Set the number of packets to be held in the outgoing queue to 10. If an ISDN connection does not exist yet, the hold-queue holds up to 10 packets before dropping them. For example:

```
SanJose(config-if)# dialer hold-queue 10
```

g. Define the load level that must be exceeded on the first ISDN B channel before the second B channel is brought up. The *load-threshold* variable represents a utilization percentage and is a number between 1 and 255, where 255 equals 100 percent.

```
SanJose(config-if)# dialer load-threshold 150 outbound
```

**Note** Enter **outbound** to calculate the load using outbound data only, **inbound** to calculate the load using inbound data only, and **either** to set the maximum calculated load as the larger of the outbound and inbound loads.

**h.** Assign this interface to dialer access group 1:

```
SanJose(config-if)# dialer-group 1
```

**i.** Configure CHAP. To configure PAP, skip this step, and go on to the next step. This command enables CHAP and specifies authentication on incoming and outgoing calls.

```
SanJose(config-if)# ppp authentication chap
```

**j.** Configure PAP. To configure CHAP, skip this step, and go to the previous step. This command enables PAP and specifies authentication on incoming and outgoing calls.

```
SanJose(config-if)# ppp authentication pap
```

**k.** Enable multilink PPP, then return to global configuration mode:

```
SanJose(config-if)# ppp multilink
SanJose(config-if)# exit
```

**Step 7** Perform this step only if ISDN calls at 64 kbps are not supported on your line. Specify the characteristics of outgoing calls from an ISDN interface by performing the following steps:

**a.** Define a class of shared configuration parameters for outgoing calls from an ISDN interface:

```
SanJose(config)# interface dialer 0
SanJose(config-if)# dialer string 5551212 class 56k
SanJose(config-if)# exit
SanJose(config)# map-class dialer 56k
```

**b.** Specify 56 kbps as the B channel speed:

```
SanJose(config-map-class)# dialer isdn speed 56
```

**c.** Change to global configuration mode:

```
SanJose(config-map-class)# exit
SanJose(config)#
```

**Step 8** If you have a Cisco 800 series router that is connected to a telephone, fax machine, or modem, configure the telephone interface by performing the following steps:

**a.** Specify the country where your router is located. For example:

```
SanJose(config)# pots country us
```

This command determines the physical characteristics of the telephone interfaces. By specifying a country, you are configuring your telephone to use country-specific default settings for each of the physical characteristics. To get a list of supported countries and the code, enter the **pots country ?** command.

**b.** Create dial peers to determine how incoming calls are routed to the telephone ports. In the following example, the dial-peer tag is 1, the ISDN local directory number (LDN) is 5551111, the telephone port is 1, and call waiting is disabled:

```
SanJose(config)# dial-peer voice 1 pots
SanJose(config-dial-peer)# destination-pattern 5551111
SanJose(config-dial-peer)# port 1
SanJose(config-dial-peer)# no call-waiting
SanJose(config-dial-peer)# exit
SanJose(config)#
```

**Note** Find out from your telephone service provider whether you need to specify an area code for the LDN.

**c.** Specify parameters for the WAN interface:

```
SanJose(config)# interface bri0
```

**d.** Specify that incoming voice calls are forwarded to the devices connected to the telephone ports:

```
SanJose(config-if)# isdn incoming-voice modem
```

## IP Routing Configuration

To configure IP routing, perform the following steps on your PC:

**Step 1** Change to global configuration mode:

```
SanJose(config-if)# exit
SanJose(config)#
```

**Step 2** Configure the router to recognize the zero subnet range as a valid range of addresses:

```
SanJose(config)# ip subnet-zero
```

**Step 3** Disable the router from translating unfamiliar words entered during a console session into IP addresses:

```
SanJose(config)# no ip domain-lookup
```

**Step 4** Configure the LAN interface by performing the following steps:

**a.** Specify parameters for the LAN interface:

```
SanJose(config)# interface ethernet0
```

**b.** Set an IP address and subnet mask for the LAN interface. For example:

```
SanJose(config)# ip address 10.1.0.1 255.255.0.0
```

**Step 5** Follow these steps to specify characteristics of the dialer rotary groups that were created earlier:

**a.** Specify parameters for the dialer rotary group:

```
SanJose(config)# interface bri0
```

**b.** Specify the IP address under the dialer group 1:

```
SanJose(config-if)# dialer-group 1
SanJose(config-if)# ip address 10.3.1.1 255.255.0.0
```

**c.** Specify that there are no IP addresses assigned for this interface:

```
SanJose(config-if)# no ip address
SanJose(config-if)#
```

**d.** To configure the WAN interface to call a site or to receive calls from a site, create a dialer map. In the following example, the same command is entered twice, once for each dial string provided for the two B channels. The next hop address is 10.3.1.2, and the host name is LosAngeles in both entries.

```
SanJose(config-if)# dialer map ip 10.3.1.2
name LosAngeles speed 56 14085553333

SanJose(config-if)# dialer map ip 10.3.1.2
name LosAngeles speed 56 14085554444
```

**Step 6** Follow these steps to configure how the IP routing protocol learns the routes:

**a.** Change to global configuration mode:

```
SanJose(config-if)# exit
SanJose(config)#
```

**b.** Configure all IP addresses to be treated as IP classless addresses:

```
SanJose(config)# ip classless
```

**c.** Set up static routes. In the following example, the LosAngeles local network is 10.2.0.0, the subnet mask is 255.255.0.0, and the router ISDN interface is 10.2.0.1:

```
SanJose(config)# ip route 10.2.0.0 255.255.0.0 10.2.1.2
```

**Note** You must configure the route to the LosAngeles network as well as the route to the LosAngeles router ISDN interface. The route to the LosAngeles router is through the dialer 0 port of the SanJose router.

**Step 7** Specify that dialer-list 1 permits dialing by the IP routing protocol:

```
SanJose(config)# dialer-list 1 protocol ip permit
```

# Corporate Router Configuration

To configure the features for this sample network, perform the following steps on your PC from global configuration mode. This section assumes that the router connected to the Cisco 800 series router is a Cisco router that supports Cisco IOS software, for example, a Cisco 3600 router. For more information, refer to the documentation that accompanied your other Cisco router.

---

**Step 1** Specify a name for the router; for example, LosAngeles:

```
router# hostname LosAngeles
```

**Step 2** Specify an encrypted password, for example, *abra cadabra*:

```
LosAngeles# enable secret abra cadabra
```

**Step 3** Specify the username of any client that will potentially dial in to your router and the password that your router and the client will share. The following example specifies *SanJose* and *gocisco1* as the username and password:

```
LosAngeles# username SanJose password gocisco1
```

**Step 4** Change to global configuration, then to interface configuration mode. Specify the ISDN switch type. To get a listing of supported switches, enter the **isdn switch-type ?** command.

```
LosAngeles# configure terminal
LosAngeles(config)# interface bri0
LosAngeles(config-if)# isdn switch-type basic-net3
```

To specify a National ISDN-1 (NI1) switch, enter the following:

```
LosAngeles(config)# isdn switch-type basic-ni1
```

**Step 5** Optional. Configure your router as a DHCP server:

**a.** Define the DHCP relay pool name. For example:

```
LosAngeles(config)# ip dhcp pool DHCPpoolLAN_0
```

**b.** Set the DHCP pool of addresses. For example:

```
LosAngeles(dhcp-config)# network 10.2.0.0 255.255.0.0
```

**c.** Set the IP addresses of the DNS servers. For example:

```
LosAngeles(dhcp-config)# dns-server 172.29.20.41 172.29.20.51
```

d. Set the Ethernet 0 IP address as the default gateway. For example:

```
LosAngeles(dhcp-config)# default-router 10.2.0.1
```

e. Exit to global configuration mode.

```
LosAngeles(dhcp-config)# exit
```

**Step 6** Configure the WAN interface by performing the following steps:

a. Specify parameters for the WAN interface:

```
LosAngeles(config)# interface bri0
```

b. Enable PPP:

```
LosAngeles(config-if)# encapsulation ppp
```

c. Enable multilink PPP:

```
LosAngeles(config-if)# ppp multilink
```

d. Create a dialer rotary group, specifying a number between 0 and 255. Dialer rotary groups are useful in environments that require multiple calling destinations. For example:

```
LosAngeles(config-if)# dialer rotary-group 0
```

e. North America only. Specify the SPID numbers assigned to your B channels, using the **isdn spid1** command for the B1 channel and the **isdn spid2** command for the B2 channel. For example:

```
LosAngeles(config-if)# isdn spid1 0155533330101
LosAngeles(config-if)# isdn spid2 0155544440101
```

f. Disable CDP.

```
LosAngeles(config-if)# no cdp enable
```

**Step 7** Specify characteristics of the dialer rotary group created earlier by following these steps:

a. Change to global configuration mode:

```
LosAngeles(config-if)# exit
LosAngeles(config)#
```

b. Create a dialer rotary group leader. Specify a number between 0 to 255 to represent your dialer rotary group.

```
LosAngeles(config)#interface dialer 0
```

**c.** Enable PPP:

```
LosAngeles(config-if)# encapsulation ppp
```

**d.** Enable DDR:

```
LosAngeles(config-if)# dialer in-band
```

**e.** Specify the amount of time (in seconds) that the line can be idle before it is disconnected. For example:

```
LosAngeles(config-if)# dialer idle-timeout 300
```

Set the number of packets to be held in the outgoing queue to 10. In the following example, if an ISDN connection does not exist yet, the hold queue holds up to 10 packets before dropping them.

```
LosAngeles(config-if)# dialer hold-queue 10
```

**f.** Define the load level that must be exceeded on the first ISDN B channel before the second B channel is brought up.The *load* variable represents a utilization percentage and is a number between 1 and 255, where 255 is 100 percent.

```
LosAngeles(config-if)# dialer load-threshold 10 outbound
```

**Note** Enter **outbound** to calculate the load using outbound data only, **inbound** to calculate the load using inbound data only, and **either** to set the maximum calculated load as the larger of the outbound and inbound loads.

**g.** Assign this interface to dialer access group 1. The dialer access group is defined later in this procedure.

```
LosAngeles(config-if)# dialer-group 1
```

**h.** Configure CHAP. To configure PAP, skip this step, and go to step i. This command enables CHAP and specifies authentication on incoming and outgoing calls.

```
LosAngeles(config-if)# ppp authentication chap
```

Configure PAP. To configure CHAP, go to step g. This command enables PAP and specifies authentication on incoming and outgoing calls.

```
LosAngeles(config-if)# ppp authentication pap
```

**i.** Enable multilink PPP:

```
LosAngeles(config-if)# ppp multilink
```

## IP Routing Configuration

To configure IP routing, perform the following steps on the PC connected to the other router.

**Step 1** Change to global configuration mode:

```
LosAngeles(config-if)# exit
LosAngeles(config)#
```

**Step 2** Specify the subnet 0.0.0.0 for your IP network:

```
LosAngeles(config)# ip subnet-zero
```

**Step 3** Disable the IP DNS-based host name-to-address translation:

```
LosAngeles(config)# no ip domain-lookup
```

**Step 4** Configure the LAN interface by performing the following steps:

**a.** Specify parameters for the LAN interface:

```
LosAngeles(config)# interface ethernet0
```

**b.** Set an IP address and subnet mask for the LAN interface. For example:

```
LosAngeles(config)# ip address 10.2.0.1 255.255.0.0
```

**Step 5** Follow these steps to specify characteristics of the dialer rotary group that were created earlier:

**a.** Change to global configuration mode:

```
LosAngeles(config-if)# exit
LosAngeles(config)#
```

**b.** Specify parameters for the dialer rotary group:

```
LosAngeles(config)# interface dialer 1
```

**c.** Set an IP address and subnet mask for this interface:

```
LosAngeles(config-if)# ip address 10.3.1.2 255.255.0.0
```

**d.** To configure the WAN interface to call a site or to receive calls from a site, create a dialer map in global configuration mode.

In this example, this command is entered twice, once for each B channel. The next hop address is 10.3.1.1, the host name is SanJose, and the dial strings are 408555111100 and 408555222200:

```
LosAngeles(config-if)# exit
LosAngeles(config)# dialer map ip 10.3.1.1 name SanJose
speed 56 408555111100
LosAngeles(config)# dialer map ip 10.3.1.1 name SanJose
speed 56 408555222200
```

**Step 6** Follow these steps to configure how the IP routing protocol learns routes:

**a.** Change to global configuration mode:

```
LosAngeles(config-if)# exit
LosAngeles(config)#
```

**b.** Set up all IP addresses to be treated as classless:

```
LosAngeles(config)# ip classless
```

**c.** Set up static routes. In the following example, the destination (San Jose) network is 10.1.0.0, the subnet mask is 255.255.0.0, and the San Jose router ISDN interface is 10.3.1.1.

```
LosAngeles(config)# ip route 10.1.0.0 255.255.0.0 10.3.1.1
```

**Note** You must configure the route to the San Jose network as well as the route to the San Jose router ISDN interface. The route to the San Jose router is through the dialer 0 port of the LosAngeles router.

**Step 7** Specify that dialer list 1 permits dialing by the IP routing protocol:

```
LosAngeles(config)# dialer-list 1 protocol ip permit
```

# Configuring Advanced Networks

This chapter describes the following configurations:

- Private IP network to Internet and corporate network
- Remote network to two corporate networks

The following features can be configured in your network:

- Dial-on-demand routing (DDR) using snapshot routing
- Leased Integrated Services Digital Network (ISDN) line
- Dynamic routing using Routing Information Protocol (RIP), including triggered extensions to RIP, and Enhanced Interior Gateway Routing Protocol (EIGRP)
- Microsoft Windows (configuring Cisco 800 series routers to function in a Windows operating system environment)
- Dynamic Host Configuration Protocol (DHCP) relay
- Dial-on-demand ISDN line activation control
- Network access restrictions
- Dial-in authentication and authorization
- X.25 on ISDN Basic Rate Interface (BRI)
- Always on/dynamic ISDN (AO/DI)
- Advanced telephone features, such as ISDN voice priority and distinctive ringing

Cisco recommends that you familiarize yourself with the features in the configuration examples to help you decide which features you wish to include in your network.

**Note** Certain protocols (IP, User Datagram Protocol [UDP], and Network Time Protocol [NTP]) send updates that can cause an ISDN line to be activated excessively. For information on preventing this situation, refer to the "Controlling the DDR ISDN Line Activation" section on page 3-26.

# Before Configuring Advanced Networks or Features

Before configuring the advanced networks or the advanced features, you must do the following:

**Step 1** Order your ISDN line from your telephone service provider. For complete information on ordering your ISDN line, see Appendix D, "Provisioning an ISDN Line."

**Step 2** While ordering your ISDN line, gather the following information from your telephone service provider:

- ISDN switch type.
- Service profile identifiers (SPIDs). In North America only, telephone service providers assign SPIDs. SPIDs identify the ISDN B channels. The SPID format is generally an ISDN telephone number with additional numbers, such as 40855522220101. Depending on the switch type that supports your ISDN line, your ISDN line could be assigned zero, one, or two SPIDs.
- ISDN local directory numbers (LDNs), which are the local ISDN telephone numbers of your routers, such as 4085552222 and 5553333.

**Note** The format of the LDN varies from region to region, depending on the telephone service provider. In some regions, you need to add the area code to the telephone number. Find out from your local telephone service provider whether or not you need to specify an area code for the LDN.

**Step 3** If you are setting up an Internet connection, gather the following information from your Internet service provider (ISP):

- PPP client name that the ISP assigns as your login name
- PPP authentication type, either Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP)
- PPP password to access your ISP account
- IP address information: the IP address and subnet mask of the ISP ISDN interface
- ISP telephone number

**Step 4** If you are setting up a connection to a corporate network, you and the network administrator of the corporate network must decide on or generate the following information for the WAN interfaces of your routers and share this information:

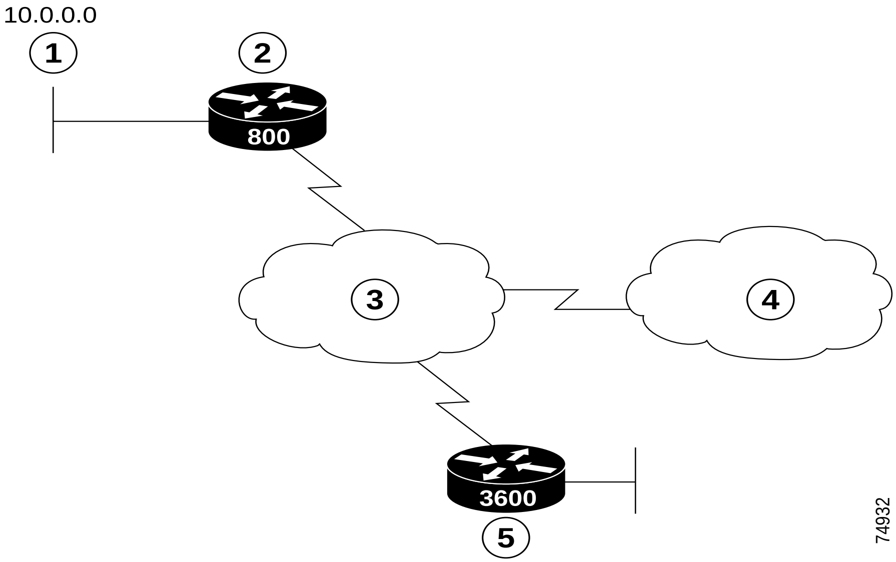
- PPP authentication type, either CHAP or PAP
- PPP client name to access the router
- PPP password to access the router
- Telephone number assigned to the telephone interface of your router

**Step 5** If you are setting up IP routing, collect information on the addressing scheme for your IP network.

# Connecting a Private IP Network to the Internet and a Corporate Network

In the network example shown in Figure 3-1 and Table 3-1, the Cisco 800 series router connects a private IP network to an ISP and a corporate network. In this network, the ISP assigns a registered IP address for the WAN interface only.

*Figure 3-1 Connecting Private IP Network to Internet and Corporate Network*



| Callout Number | Description |
|---|---|
| **1** | Private network |
| **2** | Site 1 |
| **3** | ISDN |
| **4** | Internet service provider |
| **5** | Site 2 |

# Features Used

This network uses the following features on the LAN:

- IP routing
- DHCP server (optional)

When your router is acting as a DHCP server, workstations configured as DHCP clients are automatically assigned an IP address and subnet mask.

This network uses the following features on the WAN:

- IP routing
- PPP
- NAT overload
- Internet Protocol Control Protocol (IPCP)
- CHAP or PAP over PPP

With NAT overload configured, your router can use one address for multiple hosts. With IPCP configured, your router can automatically negotiate its IP address from the router it is attempting to connect to.

You can use CHAP or PAP as the PPP authentication protocol. Cisco recommends using CHAP, because it is more secure.

For the ISDN connection, you can use one of the following options:

- DDR using snapshot routing (the ISDN line is activated only when needed)
- Permanent ISDN line lease

For complete information on these options, including how to configure them, see the "Configuring the ISDN Line" section on page 3-19.

The IP routing protocol can use either RIP or EIGRP to learn routes dynamically. You can also use triggered extensions to RIP to control when RIP sends routing updates. For information on how to configure these options, see the "Configuring Dynamic Routing" section on page 3-23.

# Configuring the Cisco 800 Series Router

**Note** Before you begin to configure your router, review the "Before Configuring Advanced Networks or Features" section on page 3-2.

Starting from global configuration mode, follow these steps to configure the Cisco 800 series router in the private IP network to connect to the Internet and the corporate network. For more information on the commands used, refer to the Cisco IOS documentation.

| | Command | Purpose |
|---|---|---|
| **Step 1** | router# **configure terminal** | Enter global configuration mode. |
| **Step 2** | router(config)# **hostname** *c804* | Enter the router name. |
| **Step 3** | c804(config)# **enable secret** *804password* | Enter the password. |
| **Step 4** | c804(config)# **pots country** *us* | Optional. If you have a Cisco 803 router that is connected to telephones, fax machines, or modems, specify the country where your router is located. Specifying a country configures the country-specific default settings for each physical characteristic. |
| **Step 5** | c804(config)# **interface bri0**<br>c804(config-if)# **isdn switch-type** *basic-ni*<br>c804(config-if) **exit** | Change to interface configuration mode, set the ISDN switch type, and return to global configuration mode. |
| **Step 6** | c804(config)# **ip subnet-zero** | Set the router to recognize the zero subnet range as a valid range of addresses. |
| **Step 7** | c804(config)# **ip dhcp pool** *DHCPpoolLAN_0* | Optional. Configure your router as a DHCP server. This step specifies the DHCP relay pool name. |
| **Step 8** | c804(dhcp-config)# **network** *10.0.0.0 255.255.255.0* | For configuring DHCP only. Set the DHCP pool of addresses. |
| **Step 9** | c804(dhcp-config)# **dns-server** *192.168.1.100* | For configuring DHCP only. Set the IP address of the DNS server. |

| | Command | Purpose |
|---|---|---|
| **Step 10** | c804(dhcp-config)# **netbios-name-server** *10.1.1.2 10.1.1.3* | For configuring DHCP only. Set the NetBIOS servers. |
| **Step 11** | c804(dhcp-config)# **default-router** *10.1.1.1* | For configuring DHCP only. Set the Ethernet 0 IP address as the default gateway. |
| **Step 12** | c804(dhcp-config)# **exit** | For configuring DHCP only. Exit to global configuration mode. |
| **Step 13** | c804(config-if)# **ip address** *10.0.0.1 255.255.255.0* | Enter the IP address and subnet mask. |
| **Step 14** | c804(config-if)# **ip nat inside**<br>c804(config-if)# **exit** | Enable Network Address Translation (NAT) on your LAN; then change to global configuration mode. |
| **Step 15** | c804(config)# **interface bri0** | Change to interface configuration mode for BRI0. |
| **Step 16** | c804(config-if)# **encapsulation ppp** | Enable PPP. |
| **Step 17** | c804(config-if)# **isdn incoming-voice modem** | Optional. Specify that incoming voice calls are forwarded to the devices connected to the telephone ports. |
| **Step 18** | c804(config-if)# **ppp authentication pap chap callin** | Enable PAP or CHAP on incoming calls only. |
| **Step 19** | c804(config-if)# **ppp chap hostname** *c804*<br>c804(config-if)# **ppp chap password** *804password* | For CHAP only. Define the router hostname and password to authenticate. |
| **Step 20** | c804(config-if)# **ppp multilink** | Enable multilink PPP. |
| **Step 21** | c804(config-if)# **ip nat outside**<br>c804(config-if)# **exit** | Configure a valid Internet address to which the inside network address will be translated, then change to global configuration mode. |
| **Step 22** | c804(config)# **interface dialer**1 | Create a dialer interface. |
| **Step 23** | c804(config-if)# **ip unnumbered ethernet0** | Specify that no specific IP addresses are assigned for Ethernet 0. |
| **Step 24** | c804(config-if)# **encapsulation ppp** | Enable PPP. |
| **Step 25** | c804(config-if)# **dialer remote-name** *corp_router* | Specify the name of the corporate router. |

| | Command | Purpose |
|---|---|---|
| **Step 26** | c804(config-if)# **dialer pool** *1* | Assign a dialer pool. |
| **Step 27** | c804(config-if)# **dialer idle-timeout** *300* | Specify the time in seconds that the line is idle before it is disconnected. |
| **Step 28** | c804(config-if)# **dialer string** *7771111* | Set up the dialer string. |
| **Step 29** | c804(config-if)# **dialer hold-queue** *10* | Specify the maximum number of packets to be held in the outgoing queue. |
| **Step 30** | c804(config-if)# **dialer load-threshold** *150* **either** | Define the load level that must be exceeded on the first ISDN B channel before the second B channel is brought up. The load-threshold variable is a number from 1 to 255 representing a utilization percentage.<br>Enter **outbound** to calculate the load using outbound data only, **inbound** to use inbound data only, and **either** to set the maximum load as the larger of the two loads. |
| **Step 31** | c804(config-if)# **dialer-group** *1* | Assign the interface to dialer access group 1. |
| **Step 32** | c804(config-if)# **ppp authentication chap pap callin** | Configure CHAP and PAP to authenticate incoming calls. |
| **Step 33** | c804(config-if)# **ppp chap hostname** *c804*<br>c804(config-if)# **ppp chap password** *804password* | Specify the CHAP host name and password. |
| **Step 34** | c804(config-if)# **ppp pap sent-username** *c804* **password** *804password* | Specify the PAP username and password. |
| **Step 35** | c804(config)# **interface dialer***2* | Create a second dialer interface. |
| **Step 36** | c804(config-if)# **ip address negotiated** | Specify that IP addresses are negotiated. |
| **Step 37** | c804(config-if)# **encapsulation ppp** | Enable PPP. |
| **Step 38** | c804(config-if)# **dialer remote-name** *isp* | Specify the name of the corporate router. |
| **Step 39** | c804(config-if)# **dialer pool** *2* | Assign a dialer pool. |
| **Step 40** | c804(config-if)# **dialer idle-timeout** *300* | Specify the time in seconds that the line is idle before it is disconnected. |
| **Step 41** | c804(config-if)# **dialer string** *18001234567* | Set up the dialer string. |

| | Command | Purpose |
|---|---|---|
| **Step 42** | c804(config-if)# **dialer hold-queue** *10* | Specify the maximum number of packets to be held in the outgoing queue. |
| **Step 43** | c804(config-if)# **dialer load-threshold** *150* **either** | Define the load level that must be exceeded on the first ISDN B channel before the second B channel is brought up. The load-threshold variable is a number from 1 to 255 representing a utilization percentage.<br>Enter **outbound** to calculate the load using outbound data only, **inbound** to use inbound data only, and **either** to set the maximum load as the larger of the two loads. |
| **Step 44** | c804(config-if)# **dialer-group** *1* | Assign the interface to dialer access group 1. |
| **Step 45** | c804(config-if)# **ppp authentication chap pap callin** | Configure CHAP and PAP to authenticate incoming calls. |
| **Step 46** | c804(config-if)# **ppp chap hostname** *generic user*<br>c804(config-if)# **password** *user pass* | Specify the CHAP username and password. |
| **Step 47** | c804(config-if)# **ppp pap sent-username** *generic_user* **password** *user pass* | Specify the PAP username and password. |
| **Step 48** | c804(config-if)# **ppp multilink** | Enable multilink PPP. |
| **Step 49** | c804(config-if)# **exit** | Change to global configuration mode. |
| **Step 50** | c804(config)# **access-list** *1* **permit** *10.0.0.1 255.255.255.0*<br>c804(config)# **dialer-list** *1* **protocol ip permit** | Specify an access list and a dialer list to control IP traffic. |
| **Step 51** | c804(config)# **ip route** *10.1.0.0 255.255.0.0 bri0* | Add a default route and interface. |
| **Step 52** | c804(config)# **dial-peer voice** *1* **pots**<br>c804(config-dial-peer)# **destination-pattern** *5551212*<br>c804(config-dial-peer)# **port** *1* | Create a dial peer to determine how incoming calls are routed to the telephone port 1. |
| **Step 53** | c804(config-dial-peer)# **exit** | Return to global configuration mode. |

| | Command | Purpose |
|---|---|---|
| **Step 54** | c804(config)# **dial-peer voice** *2* **pots**<br>c804(config-dial-peer)# **destination-pattern** *5551313*<br>c804(config-dial-peer)# **port** *2* | Create a second dial peer for the telephone port 2. |
| **Step 55** | c804(config-dial-peer)# **exit** | Change to global configuration mode. |
| **Step 56** | c804(config)# **ip nat inside source list** *1* **interface** *bri0* **overload**<br>c804(config)# **access-list** *1* **permit** *10.0.0.0 0.0.0.255* | Set global NAT commands. In this example, all inside network addresses assigned to interface BRI0 are configured for translation, and the access list that contains the inside network addresses is defined. |

# Configuring the Router at the Corporate Site

Starting from global configuration mode, follow these steps to configure the router that is connected to the Cisco 800 series router. This procedure assumes that this router is a Cisco router that supports Cisco IOS software, such as a Cisco 3600 router.

| | Command | Purpose |
|---|---|---|
| **Step 1** | router# **configure terminal** | Enter global configuration mode. |
| **Step 2** | router(config)# **hostname** *3600* | Specify a name for the router. |
| **Step 3** | 3600(config)# **enable secret** *secret* | Set an encrypted password to gain access to privileged EXEC mode commands. |
| **Step 4** | 3600(config)# **username** *c800* **password** *c800 pass* | Specify the username and password of the Cisco 800 series router. |
| **Step 5** | 3600(config)# **ip subnet-zero** | Set router to recognize the zero subnet range as a valid range of addresses. |
| **Step 6** | 3600(config)# **no ip domain-lookup** | Disable router from translating unfamiliar words entered during a console session into IP addresses. |

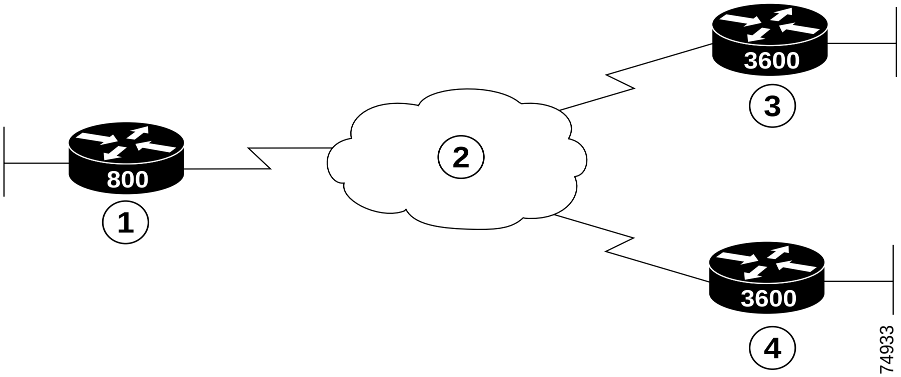
| | Command | Purpose |
|---|---|---|
| **Step 7** | 3600(config)# **ip dhcp pool** *DHCPpoolLAN_1* | Optional. Configure your router as a DHCP server. This step specifies the DHCP relay pool name. |
| **Step 8** | 3600(dhcp-config)# **network** *192.168.1.0 255.255.255.0* | For configuring DHCP only. Set the DHCP pool of addresses. |
| **Step 9** | 3600(dhcp-config)# **dns-server** *192.168.1.2* | For configuring DHCP only. Set the IP address of the DNS server. |
| **Step 10** | 3600(dhcp-config)# **netbios-name-server** *192.168.1.11 192.168.1.12* | For configuring DHCP only. Set the NetBIOS servers. |
| **Step 11** | 3600(dhcp-config)# **default-router** *192.168.1.1* | For configuring DHCP only. Set the Ethernet 0 IP address as the default gateway. |
| **Step 12** | 3600(dhcp-config)# **exit** | For configuring DHCP only. Exit to global configuration mode. |
| **Step 13** | 3600(config)# **ip local pool** *POOL1 192.168.1.10 192.168.1.20* | Set a local pool of IP addresses to be used when Cisco 800 series router attempts to connect. |
| **Step 14** | 3600(config)# **interface e0** | Change to interface configuration mode for Ethernet 0. |
| **Step 15** | *3600(config-if)#* **ip address** *192.168.1.1 255.255.255.0*<br>3600(config-if)# **exit** | Set IP address and subnet mask for the Ethernet interface, then return to global configuration mode. |
| **Step 16** | 3600(config)# **interface bri0**<br>3600(config-if)# **isdn switch-type** *basic-net3* | Change to interface configuration mode for BRI0 and specify the ISDN switch type. |
| **Step 17** | 3600(config-if)# **encapsulation ppp** | Enable PPP. |
| **Step 18** | 3600(config-if)# **isdn spid1** *0155533330101*<br>3600(config-if)# **isdn spid2** *0155544440101* | North America only. Specify SPID numbers assigned to B channels by telephone service provider. |
| **Step 19** | 3600(config-if)# **peer default ip address pool** *POOL1* | Specify address from a particular IP address pool be returned to the connected router. Use pool name specified in **ip local pool** command. |

| | Command | Purpose |
|---|---|---|
| **Step 20** | 3600(config-if)# **ppp authentication chap callin**<br>or<br>3600(config-if)# **ppp authentication pap callin** | Enable PAP or CHAP and specify authentication in incoming calls only. |
| **Step 21** | 3600(config-if)# **ppp multilink** | Enable multilink PPP. |
| **Step 22** | 3600(config-if)# **no cdp enable** | Disable CDP. |
| **Step 23** | 3600(config-if)# **exit**<br>3600(config)# **ip classless** | Change to global configuration mode, and set IP addresses to be treated as classless. |

# Connecting a Remote Network to Two Corporate Networks

In the network example shown in Figure 3-2 and Table 3-2, the Cisco 800 series router and two other routers, such as Cisco 3600 routers, connect a remote network to two corporate networks.

***Figure 3-2 Connecting Remote Network to Two Corporate Networks***



| Callout Number | Description |
|---|---|
| **1** | Site 1 |
| **2** | ISDN network |
| **3** | Site 2 |
| **4** | Site 3 |

# Features Used

This network uses the following features on the LAN:

- IP routing (Cisco recommends for management purposes, such as Telnet)
- DHCP server (optional)

When your router is acting as a DHCP server, workstations configured as DHCP clients are automatically assigned an IP address and subnet mask.

This network uses the following features on the WAN:

- IP routing
- PPP
- NAT overload
- IPCP
- CHAP or PAP over PPP

With NAT overload configured, your router can use one address for multiple hosts. With IPCP configured, your router can automatically negotiate its IP address from the router it is attempting to connect to.

You can use either CHAP or PAP as the PPP authentication protocol. Cisco recommends using CHAP because it is the more secure of the two protocols.

For the ISDN connection, you can use one of the following options:

- DDR using snapshot routing (the ISDN line is activated only when needed)
- Permanently leased ISDN line

For complete information on these options, including how to configure them, see the "Configuring the ISDN Line" section on page 3-19.

The IP routing protocol can use either RIP or EIGRP to learn routes dynamically. You can use either one of these options. You can also use triggered extensions to RIP to control when RIP sends routing updates. For information on how to configure these options, see the "Configuring Dynamic Routing" section on page 3-23.

## Configuring the Cisco 800 Series Router

**Note** Before you begin to configure your router, review the "Before Configuring Advanced Networks or Features" section on page 3-2 .

Starting from global configuration mode, follow these steps to configure the Cisco 800 series router in the remote network to two corporate networks. For information on the commands used in this table, refer to the Cisco IOS documentation.

| | Command | Purpose |
|---|---|---|
| **Step 1** | router# **configure terminal** | Enter global configuration mode. |
| **Step 2** | router(config)# **hostname** *c804* | Enter the router name. |
| **Step 3** | c804(config)# **enable secret** *804password* | Enter the password. |
| **Step 4** | c804(config)# **pots country** *us* | Optional. If you have a Cisco 803 or 804 router that are connected to telephones, fax machines, or modems, specify the country where your router is located. Specifying a country configures the country-specific default settings for each physical characteristic. |
| **Step 5** | c804(config)# **ip subnet-zero** | Set the router to recognize the zero subnet range as a valid range of addresses. |
| **Step 6** | c804(config)# **ip dhcp pool** *DHCPpoolLAN_0* | Optional. Configure your router as a DHCP server. In this step, specify the DHCP relay pool name. |
| **Step 7** | c804(dhcp-config)# **network** *192.168.1.0 255.255.255.0* | Optional. Set the DHCP pool of addresses. |

| | Command | Purpose |
|---|---|---|
| **Step 8** | c804(dhcp-config)# **dns-server** *172.29.20.41 172.29.20.51* | For DHCP configuration only. Set the IP address of the DNS servers. |
| **Step 9** | c804(dhcp-config)# **netbios-name-server** *172.29.20.41 172.29.20.51* | For DHCP configuration only. Set the NetBIOS servers. |
| **Step 10** | c804(dhcp-config)# **default-router** *192.168.1.1* | For DHCP configuration only. Set the Ethernet 0 IP address as the default gateway. |
| **Step 11** | c804(dhcp-config)# **exit** | For DHCP configuration only. Exit to global configuration mode. |
| **Step 12** | c804(config)# **interface ethernet0** | Change to the Ethernet interface configuration mode. |
| **Step 13** | c804(config-if)# **ip nat inside** | Enable NAT on the inside network. |
| **Step 14** | c804(config-if)# **ip address** *192.168.2.2 255.255.255.0*<br>c804(config-if)# **exit** | Assign the IP addresses for Ethernet 0; then change to global configuration mode. |
| **Step 15** | c804(config)# **interface dialer1** | Create a dialer interface. |
| **Step 16** | c804(config-if)# **encapsulation ppp** | Enable PPP. |
| **Step 17** | c804(config-if)# **dialer remote-name** *corp1* | Specify the name of the corporate router. |
| **Step 18** | c804(config-if)# **dialer pool** *1* | Assign a dialer pool. |
| **Step 19** | c804(config-if)# **dialer idle-timeout** *300* | Specify the time, in seconds, that the line is idle before it is disconnected. |
| **Step 20** | c804(config-if)# **dialer string** *7771111* | Set up the dialer string. |
| **Step 21** | c804(config-if)# **dialer hold-queue** *10* | Specify the maximum number of packets to be held in the outgoing queue. |
| **Step 22** | c804(config-if)# **dialer-group** *1* | Assign the interface to dialer access group 1. |
| **Step 23** | c804(config-if)# **ppp authentication chap pap callin** | Configure CHAP and PAP to authenticate incoming calls. |
| **Step 24** | c804(config-if)# **ppp chap hostname** *c804* | Specify the CHAP host name. |
| **Step 25** | c804(config-if)# **ppp chap password** *804password* | Specify the CHAP password. |
| **Step 26** | c804(config-if)# **ppp pap sent-username** *c804* **password** *804password* | Specify the PAP username and password. |

| | Command | Purpose |
|---|---|---|
| **Step 27** | c804(config)# **interface dialer2** | Create a second dialer interface. |
| **Step 28** | c804(config-if)# **ip address** *192.168.3.1 255.255.255.0* | Assign the IP addresses for Ethernet 0. |
| **Step 29** | c804(config-if)# **encapsulation ppp** | Enable PPP. |
| **Step 30** | c804(config-if)# **dialer remote-name** *corp2* | Specify the name of the corporate router. |
| **Step 31** | c804(config-if)# **dialer pool** *1* | Assign a dialer pool. |
| **Step 32** | c804(config-if)# **dialer idle-timeout** *300* | Specify the time in seconds that the line is idle before it is disconnected. |
| **Step 33** | c804(config-if)# **dialer string** *7772222* | Set up the dialer string. |
| **Step 34** | c804(config-if)# **dialer hold-queue** *10* | Specify the maximum number of packets to be held in the outgoing queue. |
| **Step 35** | c804(config-if)# **dialer-group** *2* | Assign the interface to a dialer access group. |
| **Step 36** | c804(config-if)# **ppp authentication chap pap callin** | Configure CHAP and PAP to authenticate incoming calls. |
| **Step 37** | c804(config-if)# **ppp chap hostname** *c804* | Specify the CHAP host name. |
| **Step 38** | c804(config-if)# **ppp chap password** *804password* | Specify the CHAP password. |
| **Step 39** | c804(config-if)# **ppp pap sent-username** *c804* **password** *804password* | Configure PAP username and password. |
| **Step 40** | c804(config-if)# **exit**<br>c804(config)# | Change to global configuration mode. |
| **Step 41** | c804(config)# **dialer-list** *1* **protocol ip permit**<br>c804(config) **dialer-list** *2* **protocol ip permit** | Specify dialer-list protocol permissions. |
| **Step 42** | c804(config)# **interface bri0**<br>c804(config-if)# **isdn switch-type** *basic-ni* | Change to the interface BRI0 configuration mode and set the ISDN switch type. |
| **Step 43** | c804(config-if)# **ip address** *192.168.1.1. 255.255.255.0* | Enter the IP address and subnet mask. |
| **Step 44** | c804(config-if)# **ip nat outside** | Configure a valid Internet address to which the inside network address will be translated. |

| | Command | Purpose |
|---|---|---|
| **Step 45** | c804(config-if)# **encapsulation ppp** | Enable PPP. |
| **Step 46** | c804(config-if)# **dialer rotary-group** *1*<br>c804(config-if)# **dialer rotary-group** *2* | Create dialer rotary groups 1 and 2, specifying a number between 0 and 255 for each. |
| **Step 47** | c804(config-if)# **isdn spid1 0** *4085551212*<br>c804(config-if)# **isdn spid2 0** *4085551313* | North America only. Associate the ISDN LDNs provided by your telephone service provider to the first and second SPIDs, and configure the SPID numbers to be automatically detected. |
| **Step 48** | c804(config-if)# **ppp authentication pap chap callin** | Enable PAP or CHAP for incoming data. |
| **Step 49** | c804(config-if)# **isdn incoming-voice modem** | Specify that voice calls are forwarded to the devices connected to the analog telephone ports. |
| **Step 50** | c804(config-if)# **exit** | Change to global configuration mode. |
| **Step 51** | c804(config)# **dial-peer voice** *1* **pots**<br>c804(config-dial-peer)# **destination-pattern** *5551212*<br>c804(config-dial-peer)# **port** *1* | Create a dial peer to determine how incoming calls are routed to the telephone port 1. |
| **Step 52** | c804(config-dial-peer)# **exit** | Return to global configuration mode. |
| **Step 53** | c804(config)# **dial-peer voice** *2* **pots**<br>c804(config-dial-peer)# **destination-pattern** *5551313*<br>c804(config-dial-peer)# **port** *2* | Create a second dial peer to determine how incoming calls are routed to the telephone port 2. |
| **Step 54** | c804(config-dial-peer)# **exit** | Change to global configuration mode. |
| **Step 55** | c804(config)# **ip nat inside source list** *1* **interface** *bri0* **overload**<br>c804(config)# **access-list** *1* **permit** *192.168.1.0 0.0.0.255* | Set global NAT commands. In this example, all inside network addresses assigned to interface BRI0 are configured for translation, and the access list that contains the inside network addresses is defined. |

# Configuring the Routers at the Corporate Site

Starting from global configuration mode, follow these steps to configure the routers that connect the Cisco 800 series router.

This procedure assumes that these routers are Cisco routers that support Cisco IOS software, such as a Cisco 3600 router.

| | Command | Purpose |
|---|---|---|
| Step 1 | router# **configure terminal** | Enter global configuration mode. |
| Step 2 | router(config)# **hostname** *3600* | Define the corporate router hostname. |
| Step 3 | 3600(config)# **enable secret** *secret* | Enter an encrypted password to gain access to privileged EXEC mode commands. |
| Step 4 | 3600(config)# **username** *c800* **password** *c800_pass* | Specify the username and password of the Cisco 800 series router. |
| Step 5 | 3600(config)# **ip subnet-zero** | Set router to recognize the zero subnet range as a valid range of addresses. |
| Step 6 | 3600(config)# **no ip domain-lookup** | Disable router from translating unfamiliar words entered during a console session into IP addresses. |
| Step 7 | 3600(config)# **ip local pool** *POOL1 1.1.2.1 1.1.2.7* | Set a local pool of IP addresses to be used when the Cisco 800 series router attempts to connect. Define the pool name and the range of IP addresses in the pool. |
| Step 8 | 3600(config)# **ip dhcp pool** *DHCPpoolLAN_1* | Optional if configuring your router as a DHCP server. If DHCP is not being configured, go to step 14.<br>This step specifies the DHCP relay pool name. |
| Step 9 | 3600(dhcp-config)# **network** *1.1.2.0 255.255.255.0* | For configuring DHCP only. Set the DHCP pool of addresses. |
| Step 10 | 3600(dhcp-config)# **dns-server** *1.1.2.2* | For configuring DHCP only. Set the IP address of the DNS server. |
| Step 11 | 3600(dhcp-config)# **netbios-name-server** *1.2.2.2 1.2.2.3* | For configuring DHCP only. Set the NetBIOS servers. |

| | Command | Purpose |
|---|---|---|
| **Step 12** | 3600(dhcp-config)# **default-router** *1.1.2.1* | For configuring DHCP only. Set the Ethernet 0 IP address as the default gateway. |
| **Step 13** | 3600(dhcp-config)# **exit** | For configuring DHCP only. Exit to global configuration mode. |
| **Step 14** | 3600(config)# **ip address** *1.1.1.1 255.255.255.0* | Set IP address and subnet mask. |
| **Step 15** | 3600(config)# **interface bri0**<br>3600(config-if)# **isdn switch-type** *basic-net3* | Change to interface configuration mode for BRI0 and specify ISDN switch type. |
| **Step 16** | 3600(config-if)# **encapsulation ppp** | Enable PPP. |
| **Step 17** | 3600(config-if)# **isdn spid1** *0155533330101*<br>3600(config-if)# **isdn spid2** *0155544440101* | North America only. Specify SPID numbers assigned to B channels by telephone service provider. |
| **Step 18** | 3600(config-if)# **peer default ip address pool** *POOL1* | Specify address from a particular IP address pool be returned to the connected router. Use pool name specified in **ip local pool** command. |
| **Step 19** | 3600(config-if)# **ppp authentication chap**<br>or<br>3600(config-if)# **ppp authentication pap** | Enable PAP or CHAP. |
| **Step 20** | 3600(config-if)# **ppp multilink** | Enable multilink PPP. |
| **Step 21** | 3600(config-if)# **no cdp enable** | Disable CDP. |
| **Step 22** | 3600(config-if)# **exit** | Change to global configuration mode. |
| **Step 23** | 3600(config)# **ip classless** | Set the IP addresses to be treated as classless. |

# Configuring the ISDN Line

For the ISDN line, you can use one of the following features:

- DDR using snapshot routing (the ISDN line is activated only when needed)
- Permanent ISDN line lease

This section provides further information on these features and how to configure them.

# Dial-on-Demand Routing Using Snapshot Routing

You can configure the DDR feature on your ISDN line. The ISDN line is then activated by traffic demands, including sending updates to other routers. You can configure snapshot routing to control the duration and frequency of the routing updates.

**Note** Some protocols (IP, UDP, and NTP) send updates that can cause an ISDN line to be activated excessively. For information on preventing this situation, see the "Controlling the DDR ISDN Line Activation" section on page 3-26.

## Configuration

Starting from interface configuration mode, follow these steps to configure DDR using snapshot routing. For information on the commands used in this configuration, refer to the Cisco IOS documentation.

| | Command | Purpose |
|---|---|---|
| **Step 1** | router# **configure terminal**<br>router(config)# **interface bri0** | Enter global configuration mode. Then enter interface configuration mode. |
| **Step 2** | router(config-if)# **dialer rotary-group** *1* | Create a dialer rotary-group, useful in environments that require multiple calling destinations. Only the rotary-group needs to be configured with dialer map commands. |
| **Step 3** | router(config-if)# **interface dialer** *0* | Create a dialer rotary-group leader. |
| **Step 4** | router(config-if)# **ppp multilink** | Enable multilink PPP. |
| **Step 5** | router(config-if)# **dialer in-band** | Enable DDR. |
| **Step 6** | router(config-if)# **dialer idle-timeout** *150* | Specify the amount of time that the line is idle before it is disconnected. |
| **Step 7** | router(config-if)# **dialer hold-queue** *10* | Set number of packets held in outgoing queue. |

| | Command | Purpose |
|---|---|---|
| Step 8 | router(config-if)# **dialer load-threshold** *150* **either** | Define the load level that must be exceeded on first ISDN B channel before the second B channel is brought up, and whether the load level is defined for inbound or outbound traffic, or for either type. |
| Step 9 | router(config-if)# **dialer-group** *2* | Assign interface to dialer access group. |
| Step 10 | router(config-if)# **dialer-list** *2* **protocol** *ip* **permit** | Define the traffic types that trigger and sustain an ISDN call on interfaces sharing the same dialer-group number. |
| Step 11 | router(config-if)# **map-class dialer** *class1* | Optional. Define a class of shared configuration parameters for outgoing calls. |
| Step 12 | router(config-map-class)# **dialer isdn speed** *56* | Optional. If 64-kbps calling is not supported, enter 56 kbps as speed for the B channel. |
| Step 13 | router(config-map-class)# **exit**<br>router(config)# **interface bri0** | Change to global configuration. Then change to interface configuration mode for BRI0. |
| Step 14 | router(config-if)# **dialer map** *3.3.3.3* **name** *name1 5551000* | Create a dialer map used by the WAN interface. |
| Step 15 | router(config-if)# **exit**<br>router(config)# **interface dialer***0* | Change to global configuration mode. Then change to interface configuration for dialer 0. |
| Step 16 | router(config-if)# **snapshot server** *5*<br>or<br>router(config-if)# **snapshot client** *5* | Set up one of the following options for snapshot routing:<br>• A server router and the active time interval, in minutes (from 5 to 1000)<br>• A client router, the active time interval, in minutes (from 5 to 1000), and the quiet time interval, in minutes (from 8 to 100,000) |
| Step 17 | router(config-if)# **exit**<br>router(config)# **interface bri0** | Change to global configuration mode. Then change to interface configuration for BRI0. |
| Step 18 | router(config-if)# **dialer map snapshot** *2* *5551000* | Define a dialer map for snapshot routing on a client router connected to a DDR interface. |

## Verifying the DDR Configuration

You can test your DDR configuration by making an ISDN data call through the CLI as shown in the following steps. For more information on the commands shown, refer to the Cisco IOS documentation set.

| | Command | Purpose |
|---|---|---|
| **Step 1** | router# **isdn call interface** *bri0 5551000* | Initiate the data call and specify the interface and dial string. |
| **Step 2** | router# **isdn disconnect interface** *bri0* **all** | Disconnect the data call without bringing down the interface. |

# Configuring a Leased ISDN Line

This section describes how to configure the router so that it uses the ISDN line as a leased-line connection to the routers at the corporate site. Use the following steps to ensure that the ISDN line is always active and connected to the corporate office switch. For more information, refer to the Cisco IOS documentation.

| | Command | Purpose |
|---|---|---|
| **Step 1** | router# **configure terminal** | Enter global configuration mode. |
| **Step 2** | router(config)# **isdn leased-line bri0** *128* | Configure the BRI interface to use the ISDN physical connection as a leased-line service. Select one of the following line speeds:<br>• *128* combines the two B channels at 128 kbps. Offered in Japan only.<br>• *144* combines the two B channels and D channel at 144 kbps. |

# Configuring Dynamic Routing

The IP routing protocol can use RIP or EIGRP to learn routes dynamically. You can configure either one of these options. This section also provide information on triggered extensions to RIP.

## Configuring Routing Information Protocol

RIP is a commonly used Interior Gateway Protocol (IGP) for use in small networks.

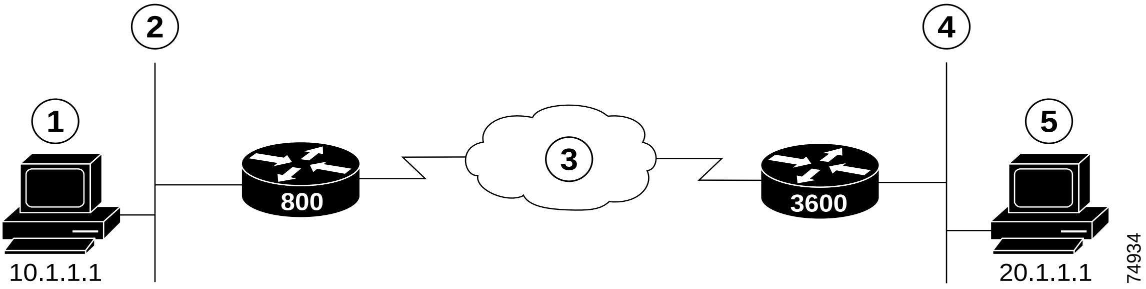
Starting in global configuration mode, follow these steps to configure RIP. For information on the commands used in this configuration, refer to the Cisco IOS documentation set.

| | Command | Purpose |
|---|---|---|
| **Step 1** | router(config)# **router rip** | Enable the RIP routing process. |
| **Step 2** | router(config-router)# **network** *network-number* | Associate a network with the RIP routing process. |
| **Step 3** | router(config-router)# **version** {**1** \| **2**} | Set the software to receive and send only RIP version 1 or only RIP version 2 packets. |

# Configuring UDP Broadcasts

Figure 3-3 and Table 3-3 show a Cisco 800 series router configured to function in a Microsoft Windows environment.

*Figure 3-3 Cisco 800 Series Router Forwarding UDP Broadcasts*



| Callout Number | Description |
|---|---|
| 1 | NT client |
| 2 | Network A |
| 3 | ISDN |
| 4 | Network B |
| 5 | NT server |

The router forwards UDP broadcasts containing PC addresses, so that PCs in network A can learn about PCs in network B, and vice versa. However, if your network uses a DDR ISDN line, the UDP broadcasts might activate this line too often.

If keeping monthly ISDN costs low is a concern, you can control when your DDR ISDN line is activated. For more information on this option, see the "Controlling the DDR ISDN Line Activation" section on page 3-26.

# Configuration of UDP Broadcasts

Starting from the ISDN interface configuration mode, use the following steps to configure the router to forward UDP broadcasts. For more information on the commands listed, refer to the Cisco IOS documentation.

| | Command | Purpose |
|---|---|---|
| **Step 1** | router# **configure terminal** | Enter global configuration mode. |
| **Step 2** | router(config)# **interface bri0** | Change to interface configuration mode for BRI0. |
| **Step 3** | router(config-if)# **ip helper-address** *address* | Set the router to forward UDP broadcasts, including broadcasts of IP addresses and IP configuration requests to the NT server. |

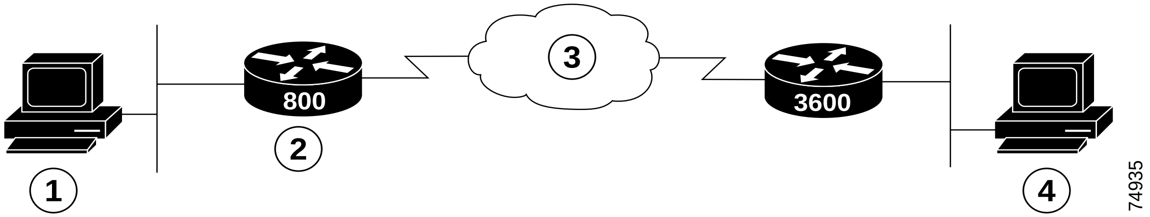
**Note** By default, eight other UDP ports, including 137 (NetBIOS name server) and 138 (NetBIOS datagram service), are enabled. For more information, refer to the Cisco IOS documentation.

# Configuring DHCP Relay

With DHCP, devices on an IP network (DHCP clients) can request configuration information from a DHCP server. DHCP allocates IP addresses from a central pool as needed.

With the DHCP relay feature configured, the Cisco 800 series routers can relay IP configuration information from the LAN interface, over the ISDN interface, and to a specified DHCP server as shown in Figure 3-4 and Table 3-4.

*Figure 3-4 DHCP Relay*



| Callout Number | Description |
|---|---|
| **1** | DHCP client |
| **2** | DHCP relay |
| **3** | ISDN network |
| **4** | DHCP server |

DHCP relay configures the router to forward UDP broadcasts, including IP configuration requests, from DHCP clients. However, if your network uses a DDR ISDN line, you might find that this line is activated excessively by the IP configuration requests and other UDP broadcasts. If keeping monthly ISDN costs low is a concern, you can control the activation of your ISDN line. For more information, refer to the "UDP Broadcasts in DHCP Relay Environment" section on page 3-28.

## Configuration of DHCP Relay

Starting in global configuration mode, use the following steps to configure DHCP relay. For more information on the commands listed, refer to the Cisco IOS documentation.

| | Command | Purpose |
|---|---|---|
| **Step 1** | router# **configure terminal** | Enter global configuration mode. |
| **Step 2** | router(config)# **ip dhcp-server** *ip-address* | Specify which DHCP server to use on your network. |

# Controlling the DDR ISDN Line Activation

The following types of traffic can activate your ISDN line and increase your monthly ISDN line cost:

- UDP broadcasts associated with networks running Microsoft Windows

- UDP broadcasts associated with networks running DHCP relay
- UDP broadcasts associated with NTP
- IP broadcasts, including RIP and EIGRP broadcasts

The following sections describe how to control these types of traffic.

# UDP Broadcasts in Windows Networks

The "Configuring UDP Broadcasts" section on page 3-23 describes how to configure the router to forward UDP broadcasts.

To control monthly costs, you can configure an extended access list so that UDP broadcasts do not activate the ISDN line. An extended access list controls packets. When defining this list, you can specify complex addresses and permit or deny specific protocols.

## Configuration of an Extended Access List

Starting in global configuration mode, use the following steps to configure an extended access list so that UDP broadcasts do not activate the ISDN line. For more information on the commands listed, refer to the Cisco IOS documentation.

| | Command | Purpose |
|---|---|---|
| **Step 1** | router# **configure terminal** | Enter global configuration mode. |
| **Step 2** | router(config)# **interface bri0** | Change to interface configuration mode for the WAN interface. |
| **Step 3** | router(config-if)# **dialer-group** *1* | Create a dialer list. |
| **Step 4** | router(config-if)# **exit** | Return to global configuration mode. |
| **Step 5** | router(config)# **access-list 100 deny udp any any eq netbios-nm** | Set NetBIOS name service packets not to activate the ISDN line. |
| **Step 6** | router(config)# **access-list 100 deny udp any any eq netbios-dgm** | Set NetBIOS datagram service packets not to activate the ISDN line. |

| | Command | Purpose |
|---|---|---|
| **Step 7** | router(config)# **access-list 100 permit ip any any** | Permit all other IP traffic. |
| **Step 8** | router(config)# **dialer-list** *1* **protocol ip list 100** | Set IP packets to activate the ISDN line. |

**Note** This example of an extended access list includes commonly anticipated restrictions. The information in this section is meant to be used as a base from which you can add or delete restrictions as appropriate for your particular network. The extended access list that you create depends on your particular network.

# UDP Broadcasts in DHCP Relay Environment

The "Configuring DHCP Relay" section on page 3-25 describes how to configure the router to forward UDP broadcasts.

To control costs, you can configure an *extended access list* so that UDP broadcasts do not activate the ISDN line. An *extended access list* controls packets. When defining this list, you can specify complex addresses and permit or deny specific protocols.

## Configuration

Starting in global configuration mode, use the following steps to configure an extended access list so that UDP broadcasts do not activate the ISDN line. For more information on the commands listed, refer to the Cisco IOS documentation.

| | Command | Purpose |
|---|---|---|
| **Step 1** | router# **configure terminal** | Enter global configuration mode. |
| **Step 2** | router(config)# **interface bri0** | Change to interface configuration mode for the WAN interface. |
| **Step 3** | router(config-if)# **dialer-group** *1* | Create a dialer list. |

| | Command | Purpose |
|---|---|---|
| Step 4 | router(config-if)# **exit** | Return to global configuration mode. |
| Step 5 | router(config)# **access-list 100 deny udp any any eq 135** | Set location services packets not to activate the ISDN line. |
| Step 6 | router(config)# **access-list 100 permit ip any any** | Permit all other IP traffic. |
| Step 7 | router(config)# **dialer-list** *1* **protocol ip list 100** | Set IP packets to activate the ISDN line. |

# UDP Broadcasts in NTP Environment

You can configure an extended access list so that UDP broadcasts associated with NTP do not activate the ISDN line. An extended access list controls packets. When defining this list, you can specify complex addresses and can permit or deny specific protocols.

## Configuration

Starting in global configuration mode, use the following steps to configure an extended access list so that UDP broadcasts associated with NTP do not activate the ISDN line. For more information on the commands listed, refer to the Cisco IOS documentation.

| | Command | Purpose |
|---|---|---|
| Step 1 | router# **configure terminal** | Enter global configuration mode. |
| Step 2 | router(config)# **interface bri0** | Specify parameters for the WAN interface. |
| Step 3 | router(config-if)# **dialer-group** *1* | Create a dialer list. |
| Step 4 | router(config-if)# **exit** | Return to global configuration mode. |
| Step 5 | router(config)# **access-list 100 deny udp any any eq ntp** | Set NTP packets not to activate the ISDN line. |

| | Command | Purpose |
|---|---|---|
| **Step 6** | router(config)# **access-list 100 permit ip any any** | Permit all other IP traffic. |
| **Step 7** | router(config)# **dialer-list** *1* **protocol ip list 100** | Specify that extended access list 100 defines which IP packets activate the ISDN line. |

# IP Traffic

You can configure an extended access list so that IP broadcasts, including RIP and EIGRP broadcasts, do not activate the ISDN line. An extended access list controls packets. When defining this list, you can specify complex addresses and permit or deny specific protocols.

## Configuration

Starting in global configuration mode, use the following steps to configure an extended access list so that IP packets do not activate the ISDN line. For more information on the commands listed, refer to the Cisco IOS documentation.

| | Command | Purpose |
|---|---|---|
| **Step 1** | router# **configure terminal** | Enter global configuration mode. |
| **Step 2** | router(config)# **interface bri0** | Change to interface configuration mode for the WAN interface. |
| **Step 3** | router(config-if)# **dialer-group** *1* | Create a dialer list. |
| **Step 4** | router(config-if)# **exit** | Return to global configuration mode. |
| **Step 5** | router(config)# **access-list 100 deny eigrp any any** | Set EIGRP packets not to activate the ISDN line. |
| **Step 6** | router(config)# **access-list 100 deny udp any any eq rip** | Set RIP packets not to activate the ISDN line. |
| **Step 7** | router(config)# **access-list 100 permit ip any any** | Allow other packets to activate the ISDN line. |

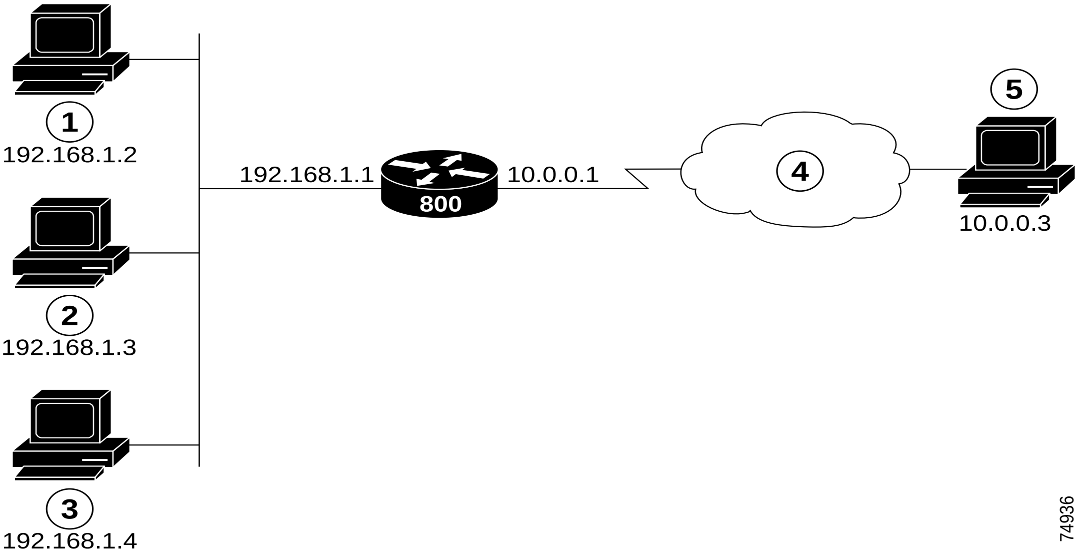
# Restricting Access to Your Network

You can restrict access to your network by creating an extended access list. An extended access list controls packets. When defining this list, you can specify complex addresses and permit or deny specific protocols.

Figure 3-5 and Table 3-5 show an example of a network with restricted access. See Table 3-1 for restrictions on network access.

**Note** This network example and extended access list include commonly anticipated restrictions. The information in this section is meant to be used as a base from which you can add or delete restrictions as they relate to your particular network. The extended access list that you create depends on your particular network.

***Figure 3-5 Restricting Access to IP Network***



| Callout Number | Description |
|---|---|
| **1** | SMTP mail server |
| **2** | Web server |
| **3** | FTP server |
| **4** | Internet service provider |
| **5** | DNS server |

*Table 3-1 Restrictions on IP Network-to-Internet Access*

| Access Permitted | Access Denied |
|---|---|
| Permit any host on network 192.168.1.0 to access any Internet host. | Prevent any Internet host from spoofing any host on the network. (*Spoofing* is illegally misrepresenting the address of the sender.) |
| Permit the outside Internet Domain Name System (DNS) server to send TCP replies to any host on the network 192.168.1.0. | Deny any Internet host from making a remote terminal connection (Telnet) to any host on network. |
| Permit the outside Internet DNS server to send UDP replies to any host on the network 192.168.1.0. | |
| Permit any Internet host to access the Simple Mail Transport Protocol (SMTP) mail server 192.168.1.2. | |
| Permit any Internet host to access the Web server 192.168.1.3. | |
| Permit any Internet host to access the File Transport Protocol (FTP) server with IP address 192.168.1.4. | |

# Configuration of Extended Access List

Starting in global configuration mode, use the following steps to set up an extended access list based on the restrictions in Table 3-1.

For information on the commands used in this table, refer to the Cisco IOS documentation.

| | Command | Purpose |
|---|---|---|
| **Step 1** | router# **configure terminal** | Enter global configuration mode. |
| **Step 2** | router(config)# **interface bri0** | Change to interface configuration mode for the WAN interface. |
| **Step 3** | router(config-if)# **dialer-group** *1* | Create a dialer list. |
| **Step 4** | router(config-if)# **exit** | Return to global configuration mode. |
| **Step 5** | router(config)# **access-list 100 permit tcp any** *192.168.1.0 0.0.0.255* **established** | Permit any host on the specified network to access any Internet host if it has an established connection. |
| **Step 6** | router(config)# **access-list 100 deny ip any** *192.168.1.0 0.0.0.255* **any** | Prevent IP spoofing using the specified network. |
| **Step 7** | router(config)# **access-list 100 permit tcp host** *10.0.0.3 192.168.1.0 0.0.0.255* **eq domain** | Permit the DNS server to send TCP replies to the specified network. |
| **Step 8** | router(config)# **access-list 100 permit udp host** *10.0.0.3 192.168.1.0 0.0.0.255* **eq domain** | Permit the DNS server to send UDP replies to the specified network. |
| **Step 9** | router(config)# **access-list 100 permit tcp any host** *192.168.1.2* **eq smtp** | Permit any host to access the mail server through SMTP. |
| **Step 10** | router(config)# **access-list 100 permit tcp any host** *192.168.1.3* **eq www** | Permit any host to access the mail server through HTTP. |
| **Step 11** | router(config)# **access-list 100 permit tcp any host** *192.168.1.4* **eq ftp** | Allow access to the FTP server from any Internet host through FTP. |
| **Step 12** | router(config)# **access-list 100 deny tcp any** *192.168.1.0 0.0.0.255* **eq telnet** | Restrict any Internet host from making a Telnet connection to any host on the specified network. |
| **Step 13** | router(config)# **interface dialer** *1* | Change to dialer interface configuration mode. |
| **Step 14** | router(config-if)# **ip access-group 100 in** | Activate access list 100. |

# Network Scenarios

This chapter provides sample network scenarios and configurations using Cisco 800 series and Cisco SOHO series routers. This chapter is useful if you are building a new network and want examples of features or configurations.

If you already have a network set up and you want to add specific features, see Chapter 7, "Router Feature Configuration."

This chapter includes the following sections:

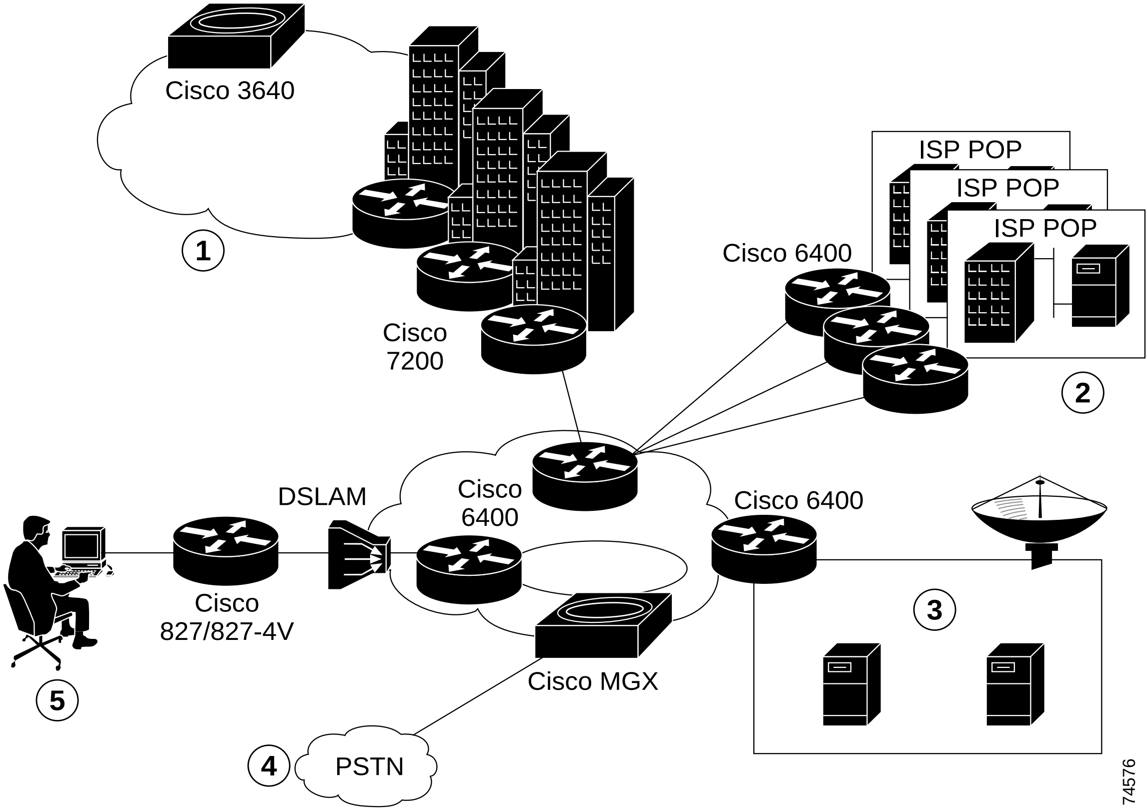
Each scenario in this chapter is described, and a network diagram and configuration network examples are provided as models on which you can pattern your network. The examples cannot, however, anticipate all of your network needs. You can choose not to use features presented in the examples, and you can choose to add or substitute features that better suit your needs.

# Cisco 827 Router Network Connections

Figure 4-1 and Table 4-1 illustrate an example of a network topology employing a Cisco 827 router connecting to the following:

- Public switched telephone network (PSTN)
- Corporate intranet
- Service provider on the Internet
- Service provider data center

*Figure 4-1 Cisco 827 Router Network Connections*



| Callout Number | Description |
|---|---|
| **1** | Corporate network connecting through a Cisco 3640 voice gateway |
| **2** | Wholesale ISP business |
| **3** | ISP POP (data center) with videoconferencing multipoint control units (MCUs) and IP/TV video servers |
| **4** | Data and voice local exchange carrier connecting through a Cisco MGX voice gateway |
| **5** | Small business or remote user, connecting to the network through a Cisco 827/827-4V router |

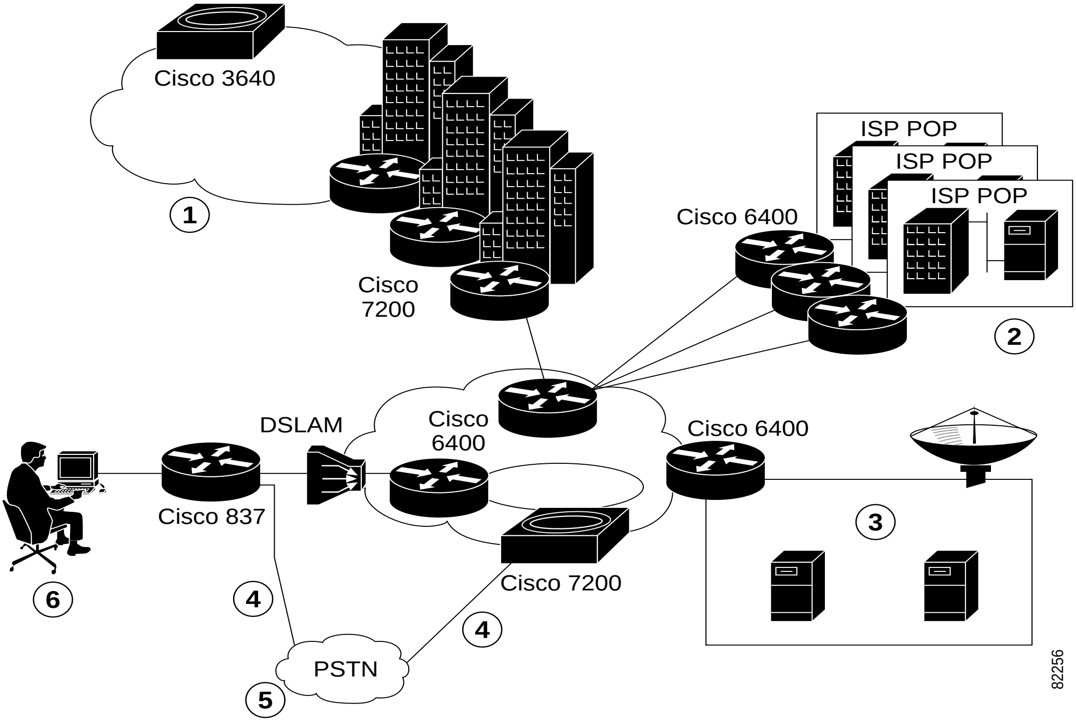
In the example, the Cisco 827 router sends data or voice packets from the remote user to the service provider or corporate network through high-speed, point-to-multipoint asymmetric digital subscriber line (ADSL) technology.

# Cisco 837 Router Network Connections

Figure 4-2 and Table 4-1 show an example of a network topology employing a Cisco 837 router connecting to the following:

- PSTN
- Corporate intranet
- Service provider on the Internet
- Service provider data center
- Dial backup and remote management

*Figure 4-2 Cisco 837 Router Network Connections*



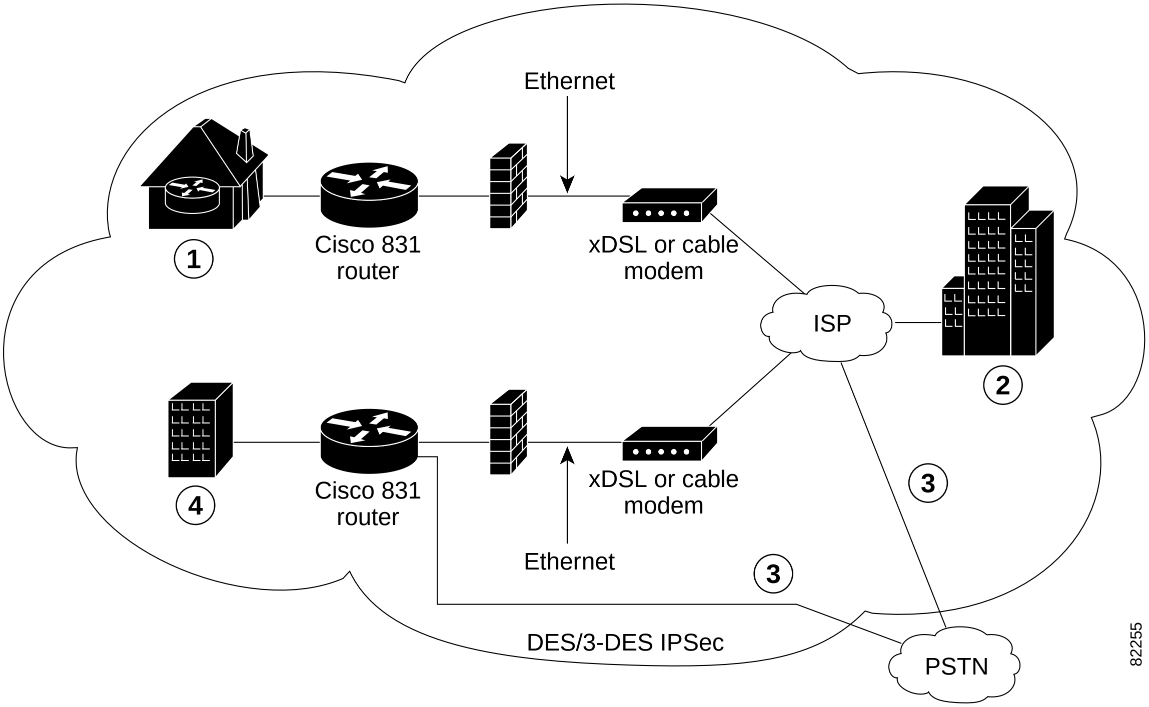
| Callout Number | Description |
|---|---|
| **1** | Corporate network connecting through a Cisco 3640 voice gateway |
| **2** | Wholesale ISP business |
| **3** | ISP POP (data center) with videoconferencing MCUs and IP/TV video servers |
| **4** | Dial backup or remote management that keeps the traffic working in case the primary line's traffic shuts down |
| **5** | PSTN to serve as an analog modem for dial backup or remote management |
| **6** | Small business or remote user, connecting to the network through a Cisco 837 router |

In the topology, the Cisco 837 router sends data packets from the remote user to the service provider or corporate network through high-speed, point-to-multipoint ADSL technology.

# Cisco 831 Router Virtual Private Network Connections

Figure 4-3 and Table 4-3 show how the Cisco 831 router can be used in a Virtual Private Network (VPN). A Cisco 831 router is linked to the ISP via a digital subscriber line (DSL) or a cable modem. Security is provided via IP security (IPSec) configuration.

***Figure 4-3 Cisco 831 Router Virtual Private Network***



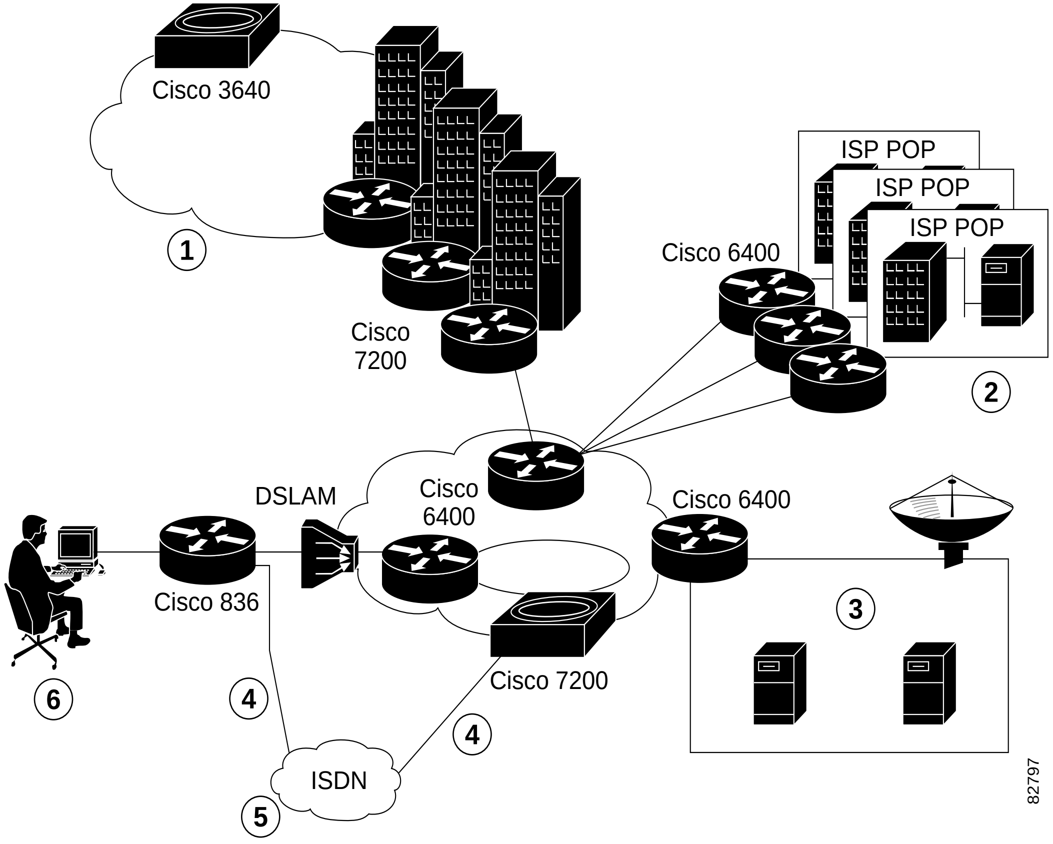
| Callout Number | Description |
|---|---|
| **1** | Small business or remote user, connecting to the network through a Cisco 831 router |
| **2** | Corporate network connecting through a Cisco router |
| **3** | Dial backup, as a failover link when primary line goes down |
| **4** | Branch office network connecting through a Cisco router |

# Cisco 836 or Cisco SOHO 96 Network Connection

Figure 4-4 and Table 4-4 show an example of a network topology employing a Cisco 836 router or a Cisco SOHO 96 router connecting to the following:

- ISDN
- Corporate intranet
- Service provider on the Internet
- Service provider data center
- Dial backup and remote management

*Figure 4-4 Cisco 836 Router Network Connections*



| Callout Number | Description |
|---|---|
| 1 | Corporate network connecting through a Cisco 3640 gateway |
| 2 | Wholesale ISP business |
| 3 | ISP POP (data center) with videoconferencing MCUs and IP/TV video servers |

| Callout Number | Description |
|---|---|
| **4** | Dial backup or remote management that keeps the traffic working in case of primary line shutdown |
| **5** | ISDN to serve as an interface for dial backup or remote management |
| **6** | Small business or remote user, connecting to the network through a Cisco 836 router |

# Internet Access Scenarios

This section provides information on the following topics related to Internet access:

- Before You Configure Your Internet Access Network
- Replacing a Bridge or Modem with a Cisco 827 Router
- PPP over Ethernet with NAT
- PPP over Ethernet with NAT Using a Dial-on-Demand PPP-over- Ethernet Connection
- PPP over ATM with NAT
- Configuring Dial Backup over the Console Port
- Configuring Dial Backup and Remote Management for the Cisco 837 and Cisco SOHO 97 Routers
- Configuring Dial Backup and Remote Management for the Cisco 836 and Cisco SOHO 96 Routers
- Configuring the DHCP Server
- Configuring the Ethernet Interface
- RFC 1483 Encapsulation with NAT
- Integrated Routing and Bridging
- Concurrent Routing and Bridging
- Data Network
- Voice Network

Each scenario is described. Also, for each scenario, a network diagram, steps for configuring network scenarios, and a configuration example are provided.

## Before You Configure Your Internet Access Network

You need to gather the following information before configuring your network for Internet access:

- Order an ADSL or G.SHDSL line from your public telephone service provider. For ADSL lines, determine that the ADSL signaling type is DMT, also called ANCII T1.413, or just DMT Issue 2. For G.SHDSL, verify that the G.SHDSL line conforms to ITU standard G.991.2 and supports Annex A, for North America, or Annex B, for Europe.
- Gather information to set up a PPP Internet connection, including the PPP client name authentication type and the PPP password.
- Determine the IP routing 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, if applicable.
- Gather DNS server IP address and default gateways.

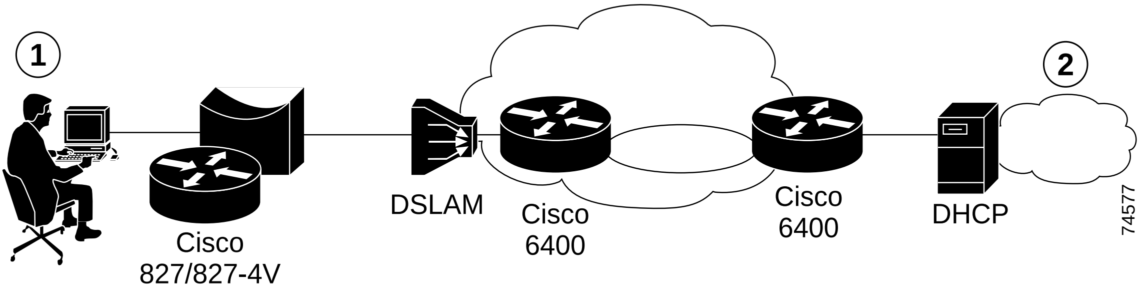
## Replacing a Bridge or Modem with a Cisco 827 Router

This scenario shows a remote user connected to the Internet. You may want to use a network similar to this one if you want to set up a minimal connection to the Internet and bridge it through the Cisco 827 routers.

This network replaces an Alcatel 1000 bridge or modem with a Cisco 827 or Cisco 827-4V router by using AAL5SNAP encapsulation and bridging (RFC 1483 bridge mode) on the ATM interface.

Figure 4-5 and Table 4-5 show the network topology for this scenario.

*Figure 4-5 Replacing a Bridge or Modem with a Cisco 827 Router*



| Callout Number | Description |
|---|---|
| **1** | Small business or remote user, connecting to the network through a Cisco 827 or Cisco 827-4V router |
| **2** | The Internet |

The Cisco 827 router is configured to act as a bridge on the WAN, so the data packets are bridged through the Cisco 6400 router onto the Internet. This network setup allows the simplicity of bridging data but also maintains router control. This network is very simple, but it limits more complex services, such as stopping broadcast traffic. If you want more services available on your network, you may want to consider some of the others scenarios in this chapter.

## Configuring the Scenario

**Note** If you have only a single ATM PVC for your bridging network, you do not have to configure the protocol bridge broadcast.

This scenario includes configuration tasks and a configuration example. To add additional features to this network, see Chapter 7, “Router Feature Configuration.”

After configuring your router, you need to configure the PVC endpoint. For a general configuration example, see the "Cisco 3640 Gateway Configuration Example" section on page 4-89.

Follow the steps below to replace a bridge or modem with the Cisco 827 router, beginning in global configuration mode. Each step includes the same values that are shown in the bridging configuration example at the end of this section.

| | Command | Task |
|---|---|---|
| Step 1 | **no ip routing** | Disable IP routing. |
| Step 2 | **bridge 1 protocol ieee** | Specify the bridge protocol to define the type of Spanning-Tree protocol. |
| Step 3 | **interface ethernet 0** | Enter configuration mode for the Ethernet interface. |
| Step 4 | **bridge-group 1** | Specify the bridge-group number to which the Ethernet interface belongs. |
| Step 5 | **no shutdown** | Enable the Ethernet interface. |
| Step 6 | **exit** | Exit configuration mode for the Ethernet interface and the router. |
| Step 7 | **interface ATM 0** | Enter configuration mode for the ATM interface. |
| Step 8 | **pvc 8/35** | Create an ATM permanent virtual circuit (PVC) for each end node with which the router communicates. |
| Step 9 | **encapsulation aal5snap** | Specify the encapsulation type for the PVC. |
| Step 10 | **bridge-group 1** | Specify the bridge-group number to which the ATM interface belongs. |
| Step 11 | **no shutdown** | Enable the ATM interface. |
| Step 12 | **exit** | Exit configuration mode for the ATM interface. |

## Configuration Example

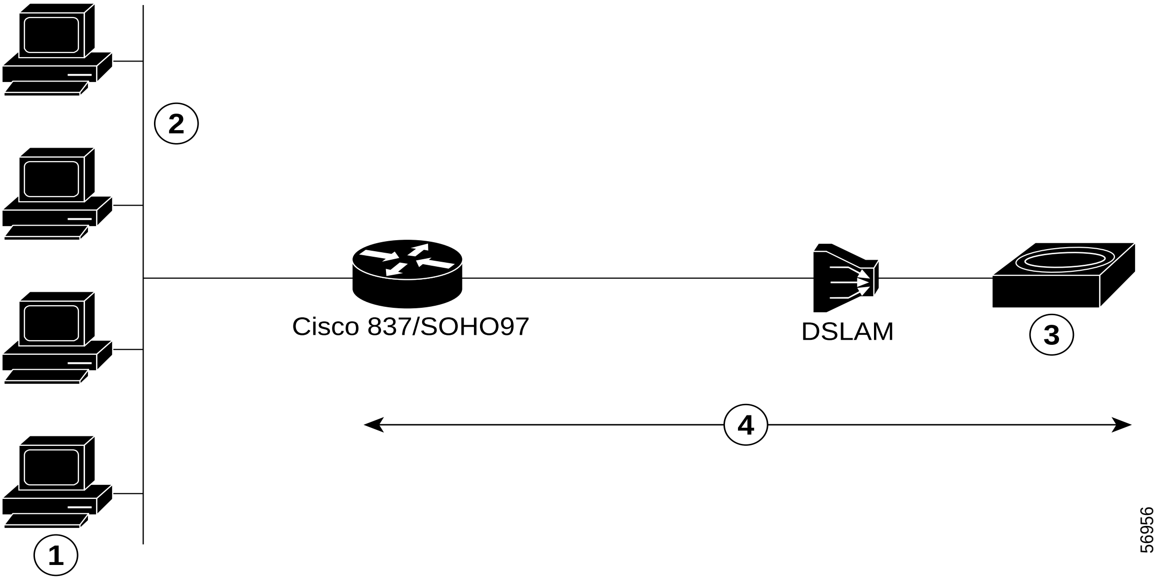
The following is a configuration example for this network scenario. You do not have to enter the commands marked "default." These commands appear automatically in the configuration file generated when you use the **show running-config** command.

```
no ip routing
!
interface Ethernet0
no ip address
no ip directed-broadcast (default)
bridge-group 1
!
interface ATM0
no ip address
no ip directed-broadcast (default)
pvc 8/35
encapsulation aal5snap
!
bridge-group 1
!
ip classless (default)
!
bridge 1 protocol ieee
!
end
```

# PPP over Ethernet with NAT

The Cisco 836 and 837 routers and the Cisco SOHO 96 and 97 routers support a PPP-over-Ethernet (PPPoE) client, with Network Addressing Translation (NAT) and with multiple PCs on the LAN. Figure 4-6 and Table 4-6 show a typical deployment scenario for PPPoE support.

*Figure 4-6 PPPoE Deployment Scenario*



| Callout Number | Description |
|---|---|
| **1** | Multiple PCs in LAN. |
| **2** | Multiple PCs connected in a LAN. |
| **3** | Access concentrator, concentrating data and LAN into ATM service over E1/T1 links. |
| **4** | PPPoE session, which is initiated on the client side by a Cisco 837 or Cisco SOHO 97 router. If the session has a timeout, or if the session is disconnected, the PPPoE client immediately attempts to reestablish the session. |

This section covers the following topics:

- Configuring the Virtual Private Dial-Up Network Group Number
- Configuring the ATM Interface
- Configuring the Dialer Interface
- Configuration Example

## Configuring the Virtual Private Dial-Up Network Group Number

Follow the steps below to configure a virtual private dial-up network (VPDN), starting in global configuration mode.

**Note** Step 1 through Step 4 are not necessary for the Cisco SOHO 96 and 97 routers.

| | Command | Task |
|---|---|---|
| **Step 1** | **vpdn enable** | Enable VPDN. |
| **Step 2** | **vpdn group** *tag* | Set the VPDN group. |
| **Step 3** | **request-dialin** | Specify the dialing direction. |
| **Step 4** | **protocol pppoe** | Specify the protocol type for the VPDN. |
| **Step 5** | **interface ATM0**<br>**mtu** *1492*<br>**pvc** *8/35* | Enter configuration mode for the ATM interface. Set the maximum transmission unit (MTU) size and PVC number. |
| **Step 6** | **pppoe-client dial-pool-number 1** | Define the pppoe client in dial pool number 1. |
| **Step 7** | **interface Dialer 1 ip address negotiated encapsulation ppp dialer-pool** *1* | Enter configuration mode for the Dialer 1 interface to obtain the IP address via IPCP. Specify the encapsulation type for the PVC using dialer pool number *1*. |

## Configuring the ATM Interface

Follow the steps below to configure the ATM interface, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **interface atm 0** | Enter configuration mode for the ATM interface. |
| Step 2 | **dsl linerate** {*number* \| **auto**} | Specify the DSL line rate. The range of valid numbers is from 72 to 2312. Note that this command is applicable only to Cisco 828 and SOHO 78 routers. |
| Step 3 | **ip address 200.200.100.1 255.255.255.0** | Set the IP address and subnet mask for the ATM interface. |
| Step 4 | **pvc** *vpi/vci* | Create an ATM PVC for each end node with which the router communcates. |
| Step 5 | **ppoe-client dial-pool-number 1** | Bind the dialer to the interface. |
| Step 6 | **no shutdown** | Enable the ATM 0 interface. |

## Configuring the Dialer Interface

Follow the steps below to configure the dialer interface, starting in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **ip route** *default-gateway-ip-address mask* **dialer** *0* | Set the IP route for the default gateway for the Dialer 0 interface. |
| Step 2 | **interface dialer 0** | Enter the Dialer 0 interface configuration. |
| Step 3 | **ip address negotiated** | Specify that the IP address is to be negotiated over PPP. |
| Step 4 | **ip mtu 1492** | Set the size of the IP maximum transmission unit (MTU). |
| Step 5 | **encapsulation ppp** | Set the encapsulation type to PPP. |

| | Command | Task |
|---|---|---|
| Step 6 | **dialer pool 1** | Specify the dialer pool to be used. |
| Step 7 | **dialer-group 1** | Assign this interface to a dialer list. |
| Step 8 | **ppp authentication chap** | Set the PPP authentication method to Challenge Handshake Authentication Protocol (CHAP). |
| Step 9 | **exit** | Exit the Dialer 0 interface configuration. |
| Step 10 | **dialer-list 1 protocol ip permit** | Create a dialer list for interested packets to be forwarded through the specified interface dialer group. |

If you enter the **clear vpdn tunnel pppoe** command with a PPPoE client session already established, the PPPoE client session terminates, and the PPPoE client immediately tries to reestablish the session.

## Configuration Example

The following example shows a configuration of a PPPoE client.

```
vpdn enable
vpdn-group 1
request-dialin
protocol pppoe
!
interface atm0
no ip address
no atm ilmi-keepalive
pvc 1/100
pppoe-client dial-pool-number 1
!
interface dialer 1
ip address negotiated
ppp authentication chap
dialer pool 1
dialer-group 1
!
dialer-list 1 protocol ip permit
```

# PPP over Ethernet with NAT Using a Dial-on-Demand PPP-over-Ethernet Connection

The Cisco 831, 836, and 837 routers and the Cisco SOHO 91, 96, and 97 routers support a PPP-over-Ethernet (PPPoE) client, using a dial-on-demand PPP-over-Ethernet connection. For a deployment scenario, see Figure 4-6 on page 4-13.

## Configuring the Virtual Private Dial-Up Network Group Number

Complete the following tasks to configure a VPDN, starting in global configuration mode.

**Note** These four steps are not necessary for the Cisco SOHO 96 and 97 routers.

| | Command | Task |
|---|---|---|
| **Step 1** | **vpdn enable** | Enable VPDN. |
| **Step 2** | **vpdn group** *tag* | Set the VPDN group. |
| **Step 3** | **request-dialin** | Specify the dialing direction. |
| **Step 4** | **protocol pppoe** | Specify the protocol type for the VPDN. |

## Configuring the ATM Interface

Follow the steps below to configure the ATM interface, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| **Step 1** | **interface atm 0** | Enter configuration mode for the ATM interface. |
| **Step 2** | **ip address 200.200.100.1 255.255.255.0** | Set the IP address and subnet mask for the ATM interface. |

| | Command | Task |
|---|---|---|
| Step 3 | **pvc** *vpi/vci* | Create an ATM PVC for each end node with which the router communicates. |
| Step 4 | **ppoe-client dial-pool-number 1 dial-on-demand** | Bind the dialer to the interface. |
| Step 5 | **no shutdown** | Enable the ATM 0 interface. |

## Configuring the Dialer Interface

Follow the steps below to configure the dialer interface, starting in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **ip route** *default-gateway-ip-address mask* **dialer** *0* | Set the IP route for the default gateway for the Dialer 0 interface. |
| Step 2 | **interface dialer 0** | Enter Dialer 0 interface configuration. |
| Step 3 | **ip address negotiated** | Specify that the IP address is to be negotiated over PPP. |
| Step 4 | *ip mtu 1492* | Set the size of the IP maximum transmission unit (MTU). |
| Step 5 | **ip nat outside** | Establish the Dialer 0 interface as the outside interface. |
| Step 6 | **encapsulation ppp** | Set the encapsulation type to PPP. |
| Step 7 | **dialer pool 1** | Specify the dialer pool to be used. |
| Step 8 | **dialer-group 1** | Assign this interface to a dialer list. |
| Step 9 | **ppp authentication chap** | Set the PPP authentication method to Challenge Handshake Authentication Protocol (CHAP). |
| Step 10 | **exit** | Exit the Dialer 0 interface configuration. |
| Step 11 | **dialer-list 1 protocol ip permit** | Create a dialer list for packets of interest to be forwarded through the interface dialer group. |

If you enter the **clear vpdn tunnel pppoe** command with a PPPoE client session already established, the PPPoE client session terminates, and the PPPoE client immediately tries to reestablish the session.

## Configuration Example

The following example shows a configuration of a PPPoE client.

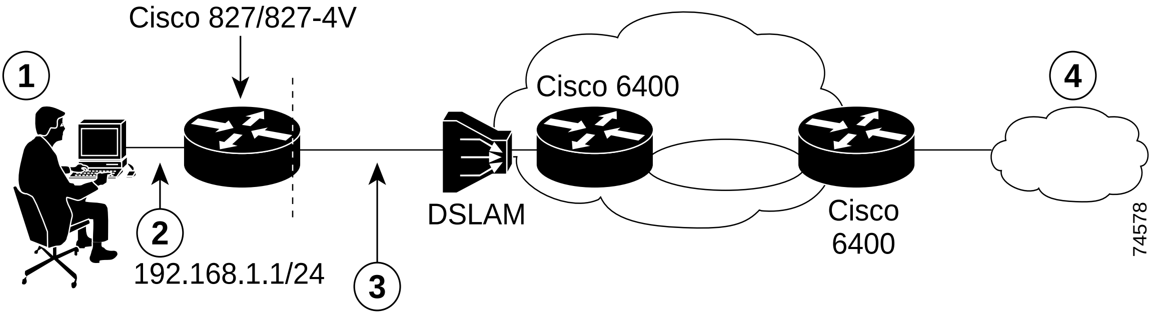
```
interface Ethernet0
 no ip address
 ip tcp adjust-mss 1400
 no keepalive
 hold-queue 100 out
!
vpdn enable
vpdn-group 1
request-dialin
protocol pppoe
!
interface atm0
no ip address
no atm ilmi-keepalive
pvc 1/100
pppoe-client dial-pool-number 1 dial-on-demand
!
interface dialer 1
ip address negotiated
ppp authentication chap
dialer pool 1
dialer-group 1
!
dialer-list 1 protocol ip permit
```

# PPP over ATM with NAT

This network shows a user connected to the Internet through PPP over ATM and one static IP address. You may want to use this scenario in your network if you want to access the network with ATM support at the endpoints. PPP over ATM provides a network solution with simplified address handling and straight user verification, as you would get in a dial network.

Figure 4-7 and Table 4-7 show the network topology for this scenario.

*Figure 4-7 PPP over ATM with NAT*



| Callout Number | Description |
|---|---|
| 1 | Small business or remote user |
| 2 | Connection to Ethernet 0 address 192.168.1.1/24 through a dialer interface |
| 3 | PPP over ATM PVC 8/35 |
| 4 | The Internet |

In this scenario, the small business or remote user on the Ethernet LAN can connect to the Internet through ADSL. The Ethernet interface carries the data packet through the LAN and offloads it to the PPP connection on the ATM interface. The dialer interface is used to connect to the Internet or the corporate office. The number of ATM PVCs is set by default.

NAT (represented as the dashed line at the edge of the Cisco 827 router) signifies two addressing domains and the inside source address. The source list defines how the packet travels through the network.

This section covers the following topics:

- Configuring the Ethernet Interface
- Configuring the Dialer Interface
- Configuring the ATM Interface

- Configuring NAT
- Configuration Example

To add other features to this network, see Chapter 7, "Router Feature Configuration."

After configuring your router, you need to configure the PVC endpoint. For a general configuration example, see the "Cisco 3640 Gateway Configuration Example" section on page 4-89.

## Configuring the Ethernet Interface

Follow the steps below to configure the Ethernet interface, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **interface ethernet 0** | Enter configuration mode for the Ethernet interface. |
| Step 2 | **ip address 192.168.1.1 255.255.255.0** | Set the IP address and subnet mask for the Ethernet interface. |
| Step 3 | **no shutdown** | Enable the interface and configuration changes just made to the Ethernet interface. |
| Step 4 | **exit** | Exit configuration mode for the Ethernet interface. |

## Configuring the Dialer Interface

Follow the steps below to configure the dialer interface, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **interface dialer 0** | Enter configuration mode for the Dialer 0 interface. |
| Step 2 | **ip address negotiated** | Configure a negotiated IP address. |

| | Command | Task |
|---|---|---|
| Step 3 | **ip nat outside** | Set the interface to be connected to the outside network. |
| Step 4 | **encapsulation ppp** | Specify the encapsulation type for the PVC to be PPP. |
| Step 5 | **dialer pool 1** | Specify which dialer pool number you are using. |
| Step 6 | **exit** | Exit configuration mode for the dialer interface. |

## Configuring the ATM Interface

Follow the steps below to configure the ATM interface, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **interface ATM 0** | Enter configuration mode for the ATM interface. |
| Step 2 | **pvc 8/35** | Create an ATM PVC for each end node with which the router communicates. |
| Step 3 | **encapsulation aal5mux ppp dialer** | Specify the encapsulation type for the PVC to be aal5mux (PPP) and point back to the dialer interface. |
| Step 4 | **dialer pool-member 1** | Specify a dialer pool member. |
| Step 5 | **no shutdown** | Enable the interface and configuration changes just made to the ATM interface. |
| Step 6 | **exit** | Exit configuration mode for the ATM interface. |

## Configuring NAT

Follow the steps below to configure NAT, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **ip nat inside source list 1 interface dialer 0 overload** | Enable dynamic translation of addresses permitted by the access list to one of addresses specified in the dialer interface. |
| Step 2 | **ip route 0.0.0.0.0.0.0.0 dialer** | Set the ip route to point to the dialer interface as a default gateway. |
| Step 3 | **access-list 1 permit 192.168.1 0 0.0.0.255** | Define a standard access list permitting addresses that need translation. |
| Step 4 | **interface ethernet 0** | Enter configuration mode for the Ethernet interface. |
| Step 5 | **ip nat inside** | Establish the Ethernet interface as the inside interface. |
| Step 6 | **no shutdown** | Enable interface and configuration changes just made to the Ethernet interface. |
| Step 7 | **exit** | Exit configuration mode for the Ethernet interface. |

## Configuration Example

In the following configuration example, you do not have to enter the commands marked “default.” These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

```
interface Ethernet0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast (default)
ip nat inside
!
interface ATM0
no ip address
no ip directed-broadcast (default)
ip nat outside
no atm ilmi-keepalive (default)
pvc 8/35
```

```
encapsulation aal5mux ppp dialer
dialer pool-member 1
!
bundle-enable
!
interface Dialer0
ip address negotiated
no ip directed-broadcast (default)
ip nat outside
encapsulation ppp
dialer pool 1
!
ip nat inside source list 1 interface Dialer0 overload
ip classless (default)
ip route 0.0.0.0 0.0.0.0 Dialer 0 (default gateway)
!
access-list 1 permit 192.168.1.0 0.0.0.255
!
end
```

# Configuring Dial Backup over the Console Port

By allowing you to configure a backup modem line connection, dial backup provides protection against WAN downtime. Dial backup is inactive until it is configured. On Cisco 831, Cisco 837, Cisco SOHO 91, and Cisco SOHO 97 routers, both the console port and the auxiliary port in the Cisco IOS software configuration are on the same physical RJ-45 port. Therefore, both ports cannot be activated simultaneously, and the command-line interface (CLI) must be used to enable or disable either one.

# Configuring Dial Backup over the ISDN Interface

Like the Cisco 831 and 837 routers and the Cisco SOHO 91 and 97 routers, the Cisco 836 router supports dial-in (for remote management) and dial-out (for dial backup) capabilities across the ISDN interface. The Cisco SOHO 96 router supports only the dial-in feature. Unlike the Cisco 831 and 837 routers and the Cisco SOHO 91 and 97 routers, the dial backup and remote management functions are configured on the Cisco 836 and Cisco SOHO 96 routers through the router’s ISDN S/T port.

**Note** The remote management described next refers to backup remote management, which function allows external control of the router via the ISDN when the ATM link goes down.

# Dial Backup Feature Limitations and Configuration

This section discusses the limitations and configuration of the dial backup feature on the Cisco 831, 836, and 837 routers and the Cisco SOHO 91, 96, and 97 routers.

## Cisco 836 and 837 Routers and Cisco SOHO 96 and 97 Routers

The following can be used to bring up the dial backup feature in the Cisco IOS software for the Cisco 836 and 837 routers and the Cisco SOHO 96 and 97 routers:

- Backup Interfaces
- Floating Static Routes
- Dialer Watch

For more information on the three features, see Chapter 1, “Concepts.”

### Backup Interfaces

When the device receives an indication that the primary line is down, the backup interface is brought up. You can configure the backup interface to go down (after a specified time) when the primary connection is restored.

The dial-on-demand routing (DDR) backup call is triggered by traffic of interest. Even if the backup interface comes out of standby mode, the router will not trigger the backup call unless it receives traffic of interest for that backup interface.

### Floating Static Routes

Floating static routes depend on traffic of interest to trigger the DDR backup call. The router does not actually trigger the backup call unless it receives traffic of interest for that backup interface, even if the router installs the floating static route in the route table.

Floating static routes are independent of line protocol status. This is an important consideration on Frame Relay circuits wherein line protocol may not go down if the data-link connection identifier (DLCI) is inactive. Floating static routes are also encapsulation independent.

**Note** When static routes are configured, the primary interface protocol must go down in order to activate the floating static route.

## Dialer Watch

Only the Extended Interior Gateway Routing Protocol (EIGRP) link-state dynamic routing protocols are supported.

There is a bottleneck in supporting bridging over console backup interfaces because bridging is not supported over slower interfaces such as console ports or auxiliary ports.

In the Cisco 836 and 837 routers, the dial backup feature is supported for the encapsulations identified in Table 4-1.

*Table 4-1 Encapsulation Types Supported by Dial Backup Feature—Cisco 836 and 837 Routers*

| Encapsulation Type (WAN) | Dial Backup Possible | Type of Dial Backup Method | Limitations |
|---|---|---|---|
| PPP over ATM<br>PPP over Ethernet | Yes | • Backup interface method<br>• Floating static routes<br>• Dialer watch | Floating static route and dialer watch need a routing protocol to run in the router. The dialer watch method brings up the backup interface as soon as the primary link goes down. The backup interface is brought down as soon as the dialer timeout is reached and the primary interface is up. Router checks the primary interface only when the dialer timeout expires. The backup interface remains up until the dialer timeout is reached, even though the primary interface is up.<br>For the dialer watch method, a routing protocol does not need to be running in the router, if the IP address of the peer is known. |
| RFC 1483 (AAL5, SNAP, and MUX) | Yes | • Backup interface method<br>• Floating static routes<br>• Dialer watch | If bridging is done through the WAN interface, it is not supported across the auxiliary port. |

## Cisco 831 and Cisco SOHO 91 Routers

Support for the dial backup feature on the Cisco 831 router is limited because the Ethernet WAN interface is always up, even when ISP connectivity is down across the modem connected to the Cisco 831 router. Support for dial backup is possible only for the PPPoE environment. The only way to bring up the backup interface is to simultaneously use the dialer watch feature. You also need to add the IP addresses of the peer in the dialer watch command and in the static route command to enable the dial backup when primary line goes down.

For the Cisco SOHO 91 router, only dial-in capability is supported.

Table 4-2 shows the encapsulation types supported by the Cisco 831 router dial backup.

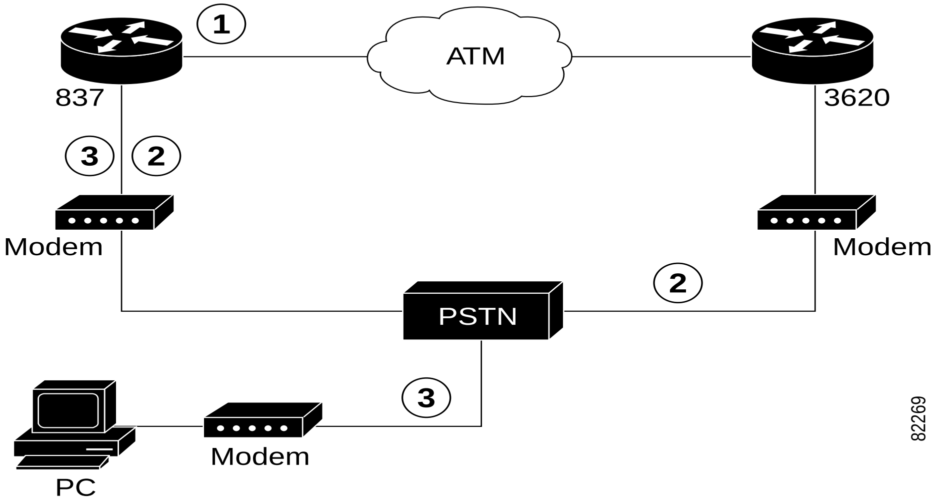
*Table 4-2 Encapsulation Types Supported by Dial Backup—Cisco 831 Router*

| Encapsulation Type | Dial Backup Possible | Type of Dial Backup Method | Limitations |
|---|---|---|---|
| PPPoE | Yes | Dialer watch | Bridging is not supported across a slow interface, for example, an auxiliary port. The peer IP address of the ISP provider is needed to configure the **dialer watch** command and the IP static route. |
| Normal IP in cable modem scenario | No | Dialer watch | The IP addresses of the peers are needed for dialer watch to work properly. If a lease time obtained by DHCP is not set short enough (one or two minutes), dial backup will not be supported. |

# Configuring Dial Backup and Remote Management for the Cisco 837 and Cisco SOHO 97 Routers

Figure 4-8 and Table 4-4 show how dial backup and remote management work in a network system when the primary line goes down.

*Figure 4-8 Cisco 837 Router Dial Backup and Remote Management*

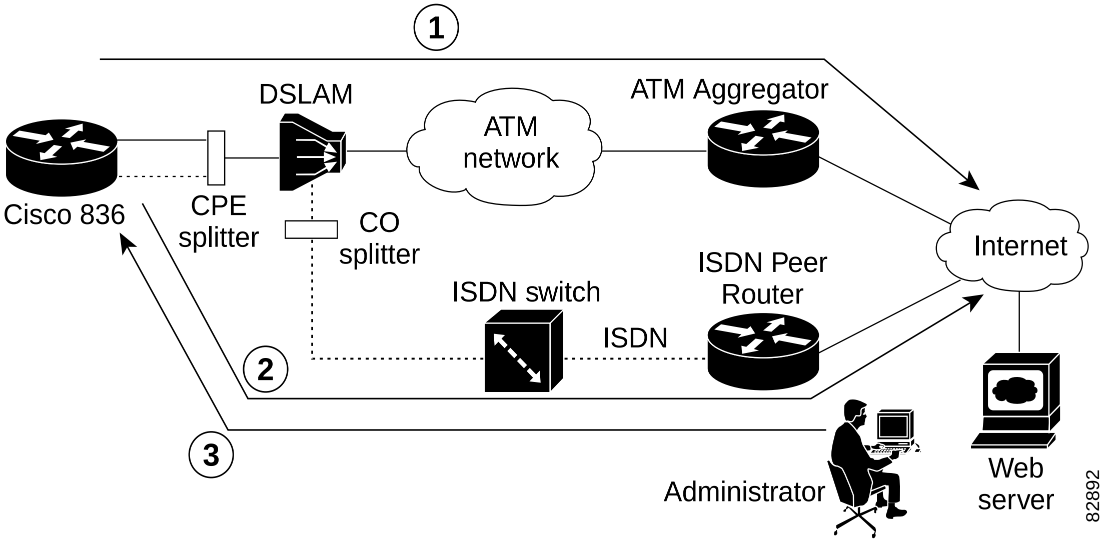


| Callout Number | Description |
|---|---|
| **1** | Main WAN link; primary connection to Internet service provider |
| **2** | Dial backup; serves as a failover link when primary line goes down |
| **3** | Remote management; serves as dial-in access to allow changes or updates to Cisco IOS configurations |

## Configuring Dial Backup and Remote Management for the Cisco 836 and Cisco SOHO 96 Routers

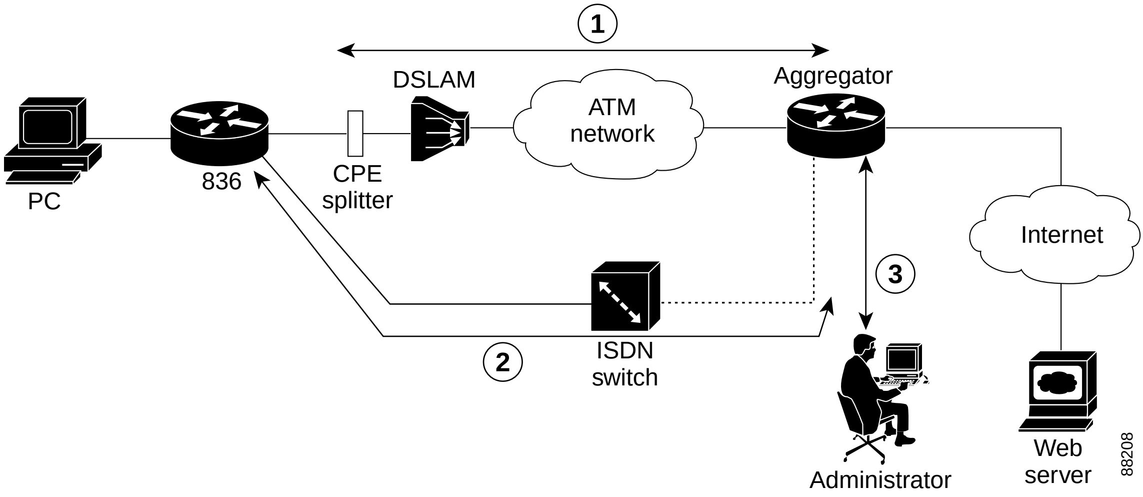
Figure 4-9, Figure 4-10, and Table 4-11 and Table 4-12 show how dial backup and remote management work in a network system when the primary line goes down. Two scenarios are typical applications of the Cisco 836 and the Cisco SOHO 96 routers. In Figure 4-9, the dial backup link goes through CPE splitter, DSLAM, and CO splitter before connecting to the ISDN switch. In Figure 4-10, the dial backup link goes directly from the Cisco 836 router to the ISDN switch.

*Figure 4-9 Cisco 836 Router Dial Backup and Remote Management—Dial Backup Through CPE Splitter, DSLAM, and CO Splitter*



| Callout Number | Description |
|---|---|
| **1** | Primary ADSL interface |
| **2** | Dial backup and remote management via ISDN interface; serves as a failover link when primary line goes down |
| **3** | Administrator remote management via ISDN interface when the primary ADSL link is down; serves as dial-in access to allow changes or updates to Cisco IOS configuration |

*Figure 4-10 Cisco 836 Router Dial Backup and Remote Management—Dial Backup Directly from Router to ISDN Switch*



| Callout Number | Description |
|---|---|
| **1** | Primary ADSL interface |
| **2** | Dial backup and remote management via ISDN interface; serves as a failover link when primary line goes down |
| **3** | Administrator remote management via ISDN interface when the primary ADSL link is down; serves as dial-in access to allow changes or updates to Cisco IOS configuration |

# PPP over ATM with Centrally Managed Addressing and with Dial Backup

When customer premises equipment such as a Cisco 837 router is connected to an ISP, an IP address is dynamically assigned to the router, or the IP address may be assigned by its peer through the centrally managed function. The dial backup feature can be added to provide a failover route in case the primary line fails.

## Configuring Dial Backup and Remote Management for the Cisco 837 Router

Follow the steps below to configure dial backup and remote management for the Cisco 837 router.

| | Command | Task |
|---|---|---|
| Step 1 | **ip name-server** *206.13.28.12* | Enter your ISP DNS IP address. |
| Step 2 | **ip dhcp pool** *1* | Configure CPE as a local DHCP server. |
| Step 3 | **vpdn enable** | Enable VPDN. |
| Step 4 | **vpdn-group** *1* | Specify VPDN group for protocol PPPoE. |
| Step 5 | **chat-script Dialout ABORT ERROR ABORT BUSY ““ “AT” OK “ATDT** *5555102* **T” TIMEOUT 45 CONNECT \c** | Configure a chat script for a modem. |
| Step 6 | **interface Async1** | Enter configuration mode for the async interface. |
| Step 7 | **interface Dialer***3* | Enter configuration mode for the dialer interface. |
| Step 8 | **dialer watch-group** *1* | Specify the group number for watch-list. |
| Step 9 | **ip nat inside source list 101 interface Dialer3 overload** | Establish the Ethernet interface as the inside interface. |
| Step 10 | **ip route 0.0.0.0 0.0.0.0 !** (*dial backup peer address @ISP*) | Set the IP route to point to the dialer interface as a default gateway. |
| Step 11 | **access-list 101 permit ip** *192.168.0.0 0.0.255.255 any* | Define an extended access list permitting addresses that need translation. |
| Step 12 | **dialer watch-list 1 ip !** *(ATM peer address @ISP) 255.255.255.255* | Evaluate the status of the primary link, based on the existence of routes to the peer. |
| Step 13 | **line con 0** | Enter configuration mode for the console interface. |
| Step 14 | **modem enable** | Change the console port to auxiliary port function. |
| Step 15 | **line aux 0** | Enter configuration mode for the auxiliary interface. |
| Step 16 | **flow control hardware** | Enable hardware signal flow control |

## Configuration Example

The following configuration example for a Cisco 837 router specifies an IP address for the ATM interface via PPP/IPCP address negotiation and dial backup over the console port.

```
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
memory-size iomem 20
enable password cisco
!
ip subnet-zero
ip name-server 206.13.28.12
ip name-server 206.13.31.12
ip name-server 63.203.35.55
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
!
ip audit notify log
ip audit po max-events 100
vpdn enable
!
vpdn-group 1
 request-dialin
  protocol pppoe
!
! 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 Ethernet0
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip tcp adjust-mss 1452
 hold-queue 100 out
!
interface ATM0
 mtu 1492
 no ip address
 no atm ilmi-keepalive
 pvc 0/35
 pppoe-client dial-pool-number 1
!
dsl operating-mode auto
!
!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
!
! 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 hasn't timeout
! Multiple routes because peer ip addresses are alternated among them
when CPE gets 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 address because peers are alternated among them
when CPE gets 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
!
! To direct traffic to an interface only if the Dialer gets assigned
with 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
!
!
line con 0
 exec-timeout 0 0
!
! Change console to aux function
 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 Dial Backup and Remote Management for the Cisco 836 Router

Follow the steps given in the "Configuring the Cisco 836 Router's ISDN Settings" section on page 4-37 to configure dial backup and remote management on the Cisco 836 router's ISDN S/T port.

## Configuring the Cisco 836 Router's ISDN Settings

The user must first configure the Cisco 836 router ISDN settings to configure the router interface as a backup interface. Follow the steps below to configure the Cisco 836 router ISDN interface as a backup interface, beginning in global configuration mode.

**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.

| | Command | Task |
|---|---|---|
| Step 1 | **isdn switch-type basic-net3** | Specify the ISDN switch type. |
| Step 2 | **interface BRI0** | Enter configuration mode for the ISDN Basic Rate Interface (BRI). |
| Step 3 | **encapsulation ppp** | Set BRI0 interface encapsulation type to PPP. |
| Step 4 | **dialer pool-member** *1* | Specify the dialer pool membership. |
| Step 5 | **isdn switch-type basic-net3** | Specify the ISDN switch type. |
| Step 6 | **exit** | Exit to return to global configuration mode. |
| Step 7 | **interface Dialer0** | Enter configuration mode for the dialer interface. |
| Step 8 | **ip address negotiated** | Obtain the IP address from the peer. |
| Step 9 | **encapsulation ppp** | Specify Dialer 0 encapsulation type as PPP. |
| Step 10 | **dialer pool 1** | Specify the dialer pool to be used. Dialer pool 1 setting associates Dialer 0 interface with BRI0 because the BRI0 dialer pool-member value is "1." |
| Step 11 | **dialer string 384040** | Specify the telephone number to be dialed. |
| Step 12 | **dialer-group 1** | Assign this interface to a dialer group. |

| | Command | Task |
|---|---|---|
| **Step 13** | **exit** | Exit to return to global configuration mode. |
| **Step 14** | **dialer-list 1 portocol ip permit** | Create a dialer list for packets of interest to be forwarded through the specified interface dialer group. Dialer-list 1 corresponds to dialer-group 1. |

# Configuring Dial Backup and Remote Management Settings

As described in the "Dial Backup Feature Limitations and Configuration" section on page 4-25, backup interface, static routes, and dialer watch are the three methods used for implementing dial backup and remote management. This section provides detailed procedures for configuring these three methods.

## Configuring Backup Interface

Follow the steps below to configure the Cisco 836 router ISDN interface as a backup interface, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| **Step 1** | **interface ATM0** | Enter ATM interface configuration mode. |
| **Step 2** | **backup interface BRI0** | Assign BRI0 as the secondary backup interface. |

## Configuring Floating Static Route

Static route and dynamic route are the two components of floating static routes. Complete the following steps to configure the static route on the Cisco 836 router ISDN port, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **ip route 0.0.0.0 0.0.0.0 22.0.0.2** | Assign the primary route. |
| Step 2 | **ip route 0.0.0.0 0.0.0.0 192.168.2.2 150** | Assign the lower routing administrative distance value for the backup interface route. 192.168.2.2 is the peer IP address of the backup interface. |

**Note** When the static routes are configured, the primary interface protocol must go down in order to activate the floating static route.

Follow the steps below to configure the dynamic route on the Cisco 836 router ISDN port, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **router rip** | Enables RIP routing. |
| Step 2 | **network 22.0.0.0** | Define the primary interface network. 22.0.0.0 is the network value of the primary interface. |
| Step 3 | **ip route 0.0.0.0 0.0.0.0 192.168.2.2 150** | Assign the lower routing administrative distance value for the backup interface route. 192.168.2.2 is the peer IP address of the backup interface. |

**Note** The floating static route depends on the routing protocol convergence times when dynamic routing is activated.

## Configuring Dialer Watch

Use the following steps to configure the dialer watch on the Cisco 836 router’s ISDN port, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **interface Dialer0** | Enter configuration mode for the dial backup interface. |
| Step 2 | **dialer watch-group 1** | Specify the group number for the watch list. |
| Step 3 | **exit** | Exit to return to global configuration mode. |
| Step 4 | **ip route 0.0.0.0 0.0.0.0 22.0.0.2** | Assign the primary route. 22.0.0.2 is the peer IP address of the primary interface. |
| Step 5 | **ip route 0.0.0.0 0.0.0.0 192.168.2.2 150** | Assign the lower routing administrative distance value for the backup interface route. 192.168.2.2 is the peer IP address of the backup interface. |
| Step 6 | **dialer watch-list 1 ip 22.0.0.2 255.255.255.255** | Assign an IP address to the watch list via the dialer watch command. If the connection on the primary interface is lost and the IP address is unavailable on the Cisco 836 router, the dial-out feature on the backup interface is triggered. 22.0.0.2 is the peer IP address of the primary interface. |

## Configuration Example

The next three configuration examples shows sample configurations for the three dial backup interface and remote management methods.

The following is an example of configuring dial backup and remote management using the backup interface command.

```
Cisco836#
!
vpdn enable
!
vpdn-group 1
 accept-dialin
 protocol pppoe
!
!Specifies the ISDN switch type
isdn switch-type basic-net3
!
interface Ethernet0
```

```
 ip address 192.168.1.1 255.255.255.0
 hold-queue 100 out
!
!ISDN interface to be used as a backup interface
interface BRI0
 no ip address
 encapsulation ppp
 dialer pool-member 1
 isdn switch-type basic-net3
!
interface ATM0
 backup interface BRI0
 no ip address
 no atm ilmi-keepalive
 pvc 1/40
   encapsulation aal5snap
   pppoe-client dial-pool-number 2
 !
 dsl operating-mode auto
!
! Dial backup interface, associated with physical BRI0 interface.
Dialer pool 1 associates it with BRI0's dialer pool member 1
interface Dialer0
 ip address negotiated
 encapsulation ppp
 dialer pool 1
 dialer idle-timeout 30
 dialer string 384040
 dialer-group 1
!
! Primary interface associated with physical ATM0's interface, dialer
pool 2 associates it with ATM0's dial-pool-number2
interface Dialer2
 ip address negotiated
 ip mtu 1492
 encapsulation ppp
 dialer pool 2
 dialer-group 2
 no cdp enable
!
ip classless
!Primary and backup interface given route metric
ip route 0.0.0.0 0.0.0.0 22.0.0.2
ip route 0.0.0.0 0.0.0.0 192.168.2.2 80
ip http server
!
!Specifies interesting traffic to trigger backup ISDN traffic
dialer-list 1 protocol ip permit
```

The following is an example of configuring dial backup and remote management using floating static routes.

```
Cisco836#
!
vpdn enable
!
vpdn-group 1
 accept-dialin
 protocol pppoe
!
!Specifies the ISDN switch type
isdn switch-type basic-net3
!
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
 hold-queue 100 out
!
!ISDN interface to be used as a backup interface
interface BRI0
 no ip address
 encapsulation ppp
 dialer pool-member 1
 isdn switch-type basic-net3
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 pvc 1/40
   encapsulation aal5snap
   pppoe-client dial-pool-number 2
 !
 dsl operating-mode auto
!
! Dial backup interface, associated with physical BRI0 interface.
Dialer pool 1 associates it with BRI0’s dialer pool member 1
interface Dialer0
 ip address negotiated
 encapsulation ppp
 dialer pool 1
 dialer idle-timeout 30
 dialer string 384040
 dialer-group 1
!
! Primary interface associated with physical ATM0’s interface, dialer
pool 2 associates it with ATM0’s dial-pool-number2
interface Dialer2
```

```
 ip address negotiated
 ip mtu 1492
 encapsulation ppp
 dialer pool 2
 dialer-group 2
!
ip classless
 no cdp enable
!Primary and backup interface given route metric (This example using 
static routes, thus atm0 line protcol must be brought down for backup 
interface to function.)
ip route 0.0.0.0 0.0.0.0 22.0.0.2
ip route 0.0.0.0 0.0.0.0 192.168.2.2 150
ip http server
!
!Specifies interesting traffic to trigger backup ISDN traffic
dialer-list 1 protocol ip permit
```

The following is an example of configuring dial backup and remote management using dialer watch.

```
Cisco836#
!
vpdn enable
!
vpdn-group 1
 accept-dialin
 protocol pppoe
!
!Specifies the ISDN switch type
isdn switch-type basic-net3
!
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
 hold-queue 100 out
!
!ISDN interface to be used as a backup interface
interface BRI0
 no ip address
 encapsulation ppp
 dialer pool-member 1
 isdn switch-type basic-net3
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 pvc 1/40
   encapsulation aal5snap
   pppoe-client dial-pool-number 2
 !
 dsl operating-mode auto
!
! Dial backup interface, associated with physical BRI0 interface.
Dialer pool 1 associates it with BRI0’s dialer pool member 1. Note
“dialer watch-group 1” associates a watch list with corresponding
“dialer watch-list” command
interface Dialer0
 ip address negotiated
 encapsulation ppp
 dialer pool 1
 dialer idle-timeout 30
 dialer string 384040
 dialer watch-group 1
 dialer-group 1
!
! Primary interface associated with physical ATM0 interface, dialer
pool 2 associates it with ATM0’s dial-pool-number2
interface Dialer2
 ip address negotiated
 ip mtu 1492
 encapsulation ppp
 dialer pool 2
 dialer-group 2
 no cdp enable
!
ip classless

!Primary and backup interface given route metric
ip route 0.0.0.0 0.0.0.0 22.0.0.2
ip route 0.0.0.0 0.0.0.0 192.168.2.2 80
ip http server
!
!Watch for interesting traffic
dialer watch-list 1 ip 22.0.0.2 255.255.255.255

!Specifies interesting traffic to trigger backup ISDN traffic
dialer-list 1 protocol ip permit
!
```

# Configuring the Aggregator and ISDN Peer Router

The aggregator is typically a concentrator router where the Cisco 836 router ATM PVC will terminate. In the configuration example shown below, the aggregator is configured as a PPPoE server to correspond with the Cisco 836 router configuration example that is given on page 4-41 and page 4-42.

The ISDN peer router is any router that has an ISDN interface and can communicate through a public ISDN network to reach the Cisco 836 router ISDN interface. The ISDN peer router provides Internet access for the Cisco 836 router during the ATM network downtime.

The following is a configuration example of an aggregator used in the Cisco 836 router network.

```
!
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
```

The following is a configuration example of an ISDN peer router used in the Cisco 836 router network.

```
!
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 Remote Management for the Cisco SOHO 97 Router

Complete the following steps to configure remote management for the Cisco SOHO 97 router.

| | Command | Task |
|---|---|---|
| Step 1 | **interface Async1** | Enter configuration mode for the async interface. |
| Step 2 | **line con 0** | Enter configuration mode for the console interface. |
| Step 3 | **modem enable** | Change the console port to the auxiliary port. |
| Step 4 | **line aux 0** | Enter configuration mode for the auxiliary interface. |
| Step 5 | **flowcontrol hardware** | Enable hardware signal flow control. |

## Configuration Example

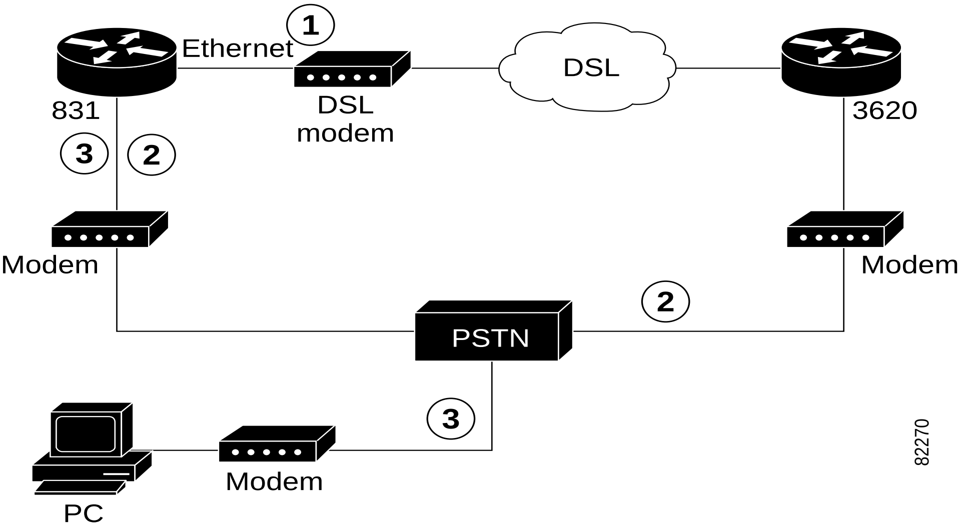
The following configuration example for a Cisco SOHO 97 router specifies the IP address for the ATM interface via PPP/IPCP address and supports dial-in maintenance over the console port.

```
!
!Remote management account
username dialin password cisco
modemcap entry MY_USR_MODEM:MSC=&F1S0=1
!
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 hold-queue 100 out
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 pvc 0/35
  encapsulation aal5mux ppp dialer
  dialer pool-member 1
 !
 dsl operating-mode auto
!
interface Async1
 no ip address
 encapsulation ppp
 dialer in-band
 autodetect encapsulation ppp
 async default routing
 async dynamic routing
 async mode dedicated
 pap authentication pap callin
 peer default ip address 192.168.2.2
!
ip nat inside source list 101 interface Dialer1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1 150
!
no ip http server
ip pim bidir-enable
!
!
access-list 101 permit ip 192.168.0.0 0.0.255.255 any
dialer-list 1 protocol ip permit
!
line con 0
 exec-timeout 0 0
 modem enable
 stopbits 1
line aux 0
 exec-timeout 0 0
 script dialer Dialout
 modem Dialin
 modem autoconfigure discovery
 transport input all
 stopbits 1
 speed 38400
 flowcontrol hardware
line vty 0 4
 login local
!
scheduler max-task-time 5000
end
```

# Configuring Dial Backup and Remote Management for Cisco 831 Router and Cisco SOHO 91 Router

Figure 4-11 and Table 4-13 show how dial backup and remote management work in a DSL modem environment when the primary line goes down. Note that the cable modem environment is currently not supported.

*Figure 4-11 Cisco 831 Router Dial Backup and Remote Management in a DSL Modem Environment*



| Callout Number | Description |
|---|---|
| **1** | Main WAN link; primary connection to Internet service provider |
| **2** | Dial backup; serves as a failover link when primary line goes down |
| **3** | Remote management; serves as a dial-in access to allow change or update of Cisco IOS configurations |

Follow the steps below to configure dial backup and remote management for the Cisco 831 router.

| | Command | Task |
|---|---|---|
| **Step 1** | **ip name-server** *206.13.28.12* | Enter your ISP DNS IP address. |
| **Step 2** | **ip dhcp pool** *1* | Configure CPE as a local DHCP server. |
| **Step 3** | **vpdn enable** | Enable VPDN. |
| **Step 4** | **vpdn-group** *1* | Specify VPDN group for protocol PPPoE. |

| | Command | Task |
|---|---|---|
| Step 5 | **chat-script Dialout ABORT ERROR ABORT BUSY ““ “AT” OK “ATDT** *5555102* **T” TIMEOUT 45 CONNECT \c** | Configure a chap script for a modem. |
| Step 6 | **interface Async1** | Enter configuration mode for the async interface. |
| Step 7 | **interface Dialer***3* | Enter configuration mode for the dialer interface. |
| Step 8 | **ip nat inside source list 101 interface Dialer3 overload** | Establish the Ethernet interface as the inside interface. |
| Step 9 | **ip route 0.0.0.0 0.0.0.0 !** *(dial backup peer address @ISP)* | Set the IP route to point to the dialer interface as a default gateway. |
| Step 10 | **access-list 101 permit ip** *192.168.0.0 0.0.255.255 any* | Define an extended access list permitting addresses that need translation. |
| Step 11 | **dialer watch-list 1 ip !** *(peer address @ISP) 255.255.255.255* | Evaluate the status of the primary link, based on the existence of routes to the peer. |
| Step 12 | **line con 0** | Enter configuration mode for the console interface. |
| Step 13 | **modem enable** | Change the console port to the auxiliary port. |
| Step 14 | **line aux 0** | Enter configuration mode for the auxiliary interface. |
| Step 15 | **flowcontrol hardware** | Enable hardware signal flow control. |

## Configuration Example for the Cisco 831 Router

The following example configures dial backup and remote management on a Cisco 831 router.

```
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
```

```
memory-size iomem 20
enable password cisco
!
ip subnet-zero
ip name-server 206.13.28.12
ip name-server 206.13.31.12
ip name-server 63.203.35.55
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
!
ip audit notify log
ip audit po max-events 100
vpdn enable
!
vpdn-group 1
 request-dialin
  protocol pppoe
!
! 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 Ethernet0
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip tcp adjust-mss 1452
 hold-queue 100 out
!
interface Ethernet1
 no ip address
 no ip route-cache
 no ip mroute-cache
 pppoe enable
 pppoe-client dial-pool-number 1
!
!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
!
! Primary wan link
interface Dialer1
 ip address negotiated
 ip mtu 1492
 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 hasn’t timeout
```

```
! Multiple routes because peer ip address are alternated among them
when CPE gets 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 CPE gets 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
!
! To direct traffic to an interface only if the Dialer gets assigned
with an ip address
route-map main permit 10
 match ip address 101
 match interface Dialer1
!
route-map backup permit 10
 match ip address 103
 match interface Dialer3
!
!
line con 0
 exec-timeout 0 0
!
! Change console to aux function
 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 Remote Management for the Cisco SOHO 91 Router

Follow the steps below to configure remote management for the Cisco SOHO 91 router.

| | Command | Task |
|---|---|---|
| **Step 1** | **interface Async1** | Enter configuration mode for the async interface. |
| **Step 2** | **line con 0** | Enter configuration mode for the console interface. |
| **Step 3** | **modem enable** | Change the console port to the auxiliary port. |
| **Step 4** | **line aux 0** | Enter configuration mode for the auxiliary interface. |
| **Step 5** | **flowcontrol hardware** | Enable hardware signal flow control. |

## Configuration Example

The following example shows how to configure a Cisco SOHO 91 router to obtain the IP address for ATM interface via PPP/IPCP address negotiation and shows how to configure and support dial-in maintenance over the console port.

```
!
!Remote management account
username dialin password cisco
modemcap entry MY_USR_MODEM:MSC=&F1S0=1
!
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 hold-queue 100 out
!
interface Async1
 no ip address
 encapsulation ppp
 dialer in-band
 autodetect encapsulation ppp
 async default routing
 async dynamic routing
 async mode dedicated
 pap authentication pap callin
 peer default ip address 192.168.2.2
!
ip nat inside source list 101 interface Dialer1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1 150
!
no ip http server
ip pim bidir-enable
!
!
access-list 101 permit ip 192.168.0.0 0.0.255.255 any
dialer-list 1 protocol ip permit
!
line con 0
 exec-timeout 0 0
 modem enable
 stopbits 1
line aux 0
 exec-timeout 0 0
 script dialer Dialout
 modem Dialin
 modem autoconfigure discovery
 transport input all
 stopbits 1
 speed 38400
 flowcontrol hardware
line vty 0 4
 login local
!
```

```
scheduler max-task-time 5000
end
```

# Configuring the DHCP Server

Dynamic Host Configuration Protocol (DHCP) is an industry-standard protocol for automatically assigning IP configurations to workstations. DHCP uses a client-server model for address allocation. As administrator, you can configure one or more DHCP servers to provide 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. The DHCP protocol is described in RFC 2131.

When configuring a DHCP server, you must configure the server properties, policies, and associated DHCP options.

**Note** Whenever you change server properties, you must reload the server to load the configuration data from the Network Registrar database.

To configure the DHCP server, you must accept Network Registrar's defaults or supply the data explicitly:

- The IP address of the server's *interface* (Ethernet card). This interface must have a static IP address that is not assigned dynamically by DHCP.
- The *subnet mask*, which identifies the network membership of the interface. The subnet mask defaults to the appropriate value, based on the network class of the interface address. In most cases, the subnet mask is 255.255.255.0.

Network Registrar uses the interface named *default* to provide configurable default values for interfaces that the DHCP server discovers automatically. If you delete the default interface, the DHCP server uses hard-coded default values for port numbers and socket buffer sizes for the interfaces that it autodiscovers.

If you enable discover-interfaces, the DHCP server uses the operating system platform support to enumerate all the active interfaces on the machine and (unless there is an interface configuration with the *ignore* feature enabled) attempts to listen on all of these. If you disable discover-interfaces, the DHCP server listens on the interface that you specify, as long as it does not have the *ignore* feature enabled.

Use the **dhcp-interface** commands to add, remove, and list the IP addresses of your server's hardware cards. Interfaces are named with the IP address and net mask for the physical device.

If you have two interface cards for the server host, use two **dhcp-interface create** commands to register them both. Use the net mask suffix 16 or 24 as part of the address.

```
nrcmd> dhcp-interface 192.168.1.12/24 create
nrcmd> dhcp-interface 10.1.2.3/24 create
```

Use the **dhcp-interface set ignore=true** command if you want Network Registrar to use only one interface, you have to set all the other ones to be ignored.

```
nrcmd> dhcp-interface 10.1.2.3/24 set ignore=true
```

## Configuring the Ethernet Interface

Follow the steps below to configure the Ethernet interface, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **interface ethernet 0** | Enter configuration mode for the Ethernet interface. |
| Step 2 | **ip address** *ip-address mask* | Set the IP address and subnet mask for the Ethernet interface. |
| Step 3 | **no shutdown** | Enable the Ethernet interface to change the state from administratively down to up. |
| Step 4 | **exit** | Exit configuration mode for the Ethernet interface. |

For complete information on the Ethernet commands, refer to the Cisco IOS Release 12.0 documentation set. For more general information on Ethernet concepts, see Chapter 1, "Concepts."

## Dynamic Addressing Received via IPCP

Use the **ip address negotiated** interface command to enable a Cisco router to automatically negotiate its own registered WAN interface IP address from a central server (via PPP/IPCP). Use the same command to enable all remote hosts to use this single registered IP address to access the global Internet. The following example shows an IPCP configuration.

```
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 pvc 0/35
  encapsulation aal5mux ppp dialer
  dialer pool-member 1
 !
 dsl operating-mode auto
!
interface Dialer1
 ip address negotiated
 ip nat outside
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 ppp authentication pap callin
 ppp pap sent-username ! USER SPECIFIC password ! USER SPECIFIC
 ppp ipcp dns request
 ppp ipcp wins request
 ppp ipcp mask request
!
```

## Configuring the Central Cisco 3620

The following example configures peer and dial backup on the Cisco 3620 router.

```
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
enable secret password
!
hostname c3620
!
boot system flash slot0:c3620-jk2o3s-mz.121-5.3.T
```

```
logging rate-limit console 10 except errors
!
username ISP password ISP
ip subnet-zero
ip name-server !ISP
ip name-server !ISP
ip name-server !ISP
!
no ip finger
!
ip audit notify log
ip audit po max-events 100
ip audit smtp spam 25111
no ip dhcp-client network-discovery
vpdn enable
no vpdn logging
!
vpdn-group 1
 accept-dialin
  protocol pppoe
  virtual-template 2
!
!
!
chat-script Dialout ABORT ERROR ABORT BUSY "" "AT" OK "ATDT 5555101\T"
TIMEOUT 45 CONNECT \c
!
modemcap entry MY_USR_MODEM:MSC=&F1S0=1
!
call rsvp-sync
!
!
interface Loopback1
 ip address 21.0.0.2 255.255.255.0
!
interface Loopback2
 ip address 22.0.0.2 255.255.255.0
!
interface Ethernet0/0
 no ip address
 half-duplex
 no cdp enable
!
interface Ethernet0/1
 no ip address
 no ip route-cache
 no ip mroute-cache
 half-duplex
 no cdp enable
!
interface ATM1/0
 no ip address
 no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
 pvc 1/40
  encapsulation aal5mux ppp Virtual-Template1
 !
!
interface ATM1/0.2 point-to-point
 pvc 1/41
  encapsulation aal5snap
  protocol pppoe
 !
!
interface Virtual-Template1
 ip unnumbered Loopback1
 peer default ip address pool test
!
interface Virtual-Template2
 ip unnumbered Loopback2
 ip mtu 1492
!
interface Async65
 no ip address
 encapsulation ppp
 dialer in-band
 dialer pool-member 1
 autodetect encapsulation ppp
 async default routing
 async dynamic routing
 async mode dedicated
!
interface Dialer0
 ip unnumbered Async65
 encapsulation ppp
 dialer pool 1
 dialer remote-name c837
 dialer string 5555101 modem-script Dialout
 dialer-group 1
 autodetect encapsulation ppp
 no cdp enable
!
ip local pool test 21.0.0.10 21.0.0.200
ip kerberos source-interface any
ip classless
```

```
no ip http server
!
dialer-list 1 protocol ip permit
no cdp run
!
!
dial-peer cor custom
!
!
!
!
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
 exec-timeout 0 0
 no activation-character
 script dialer Dialout
 no vacant-message
 modem InOut
 modem autoconfigure type MY_USR_MODEM
 transport input all
 transport output telnet
 escape-character NONE
 autohangup
 stopbits 1
 speed 38400
 flowcontrol hardware
line vty 0 4
 exec-timeout 0 0
login
!
end
```

## Configuring the Central RADIUS Server

Remote Authentication Dial-In User Service (RADIUS) enables you to secure your network against unauthorized access. A RADIUS server must be configured in the service provider or corporate network in order for a Cisco 800 series router to use RADIUS client features.

To configure RADIUS on your Cisco 800 series router, you must perform the following tasks:

- Use the **aaa new-model** global configuration command to enable authentication, authorization, and accounting (AAA). AAA must be configured if you plan to use RADIUS.
- Use the **aaa authentication** global configuration command to define the method lists for RADIUS authentication.
- Use line and interface commands to enable the defined method lists to be used.

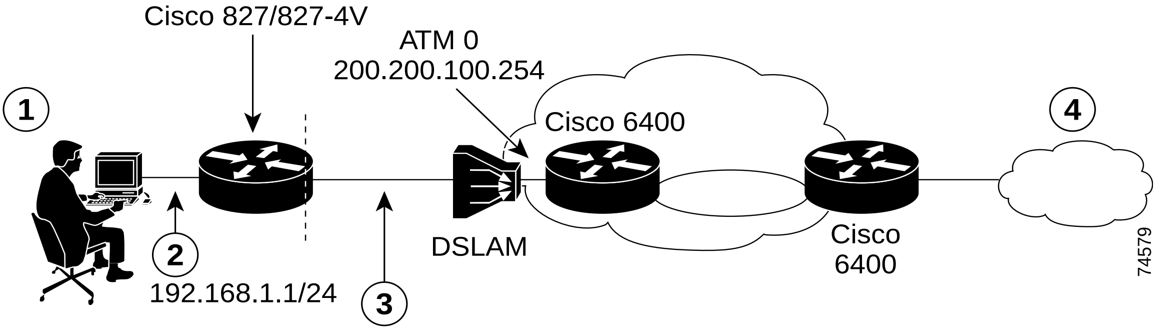
For instructions on configuring a RADIUS client, refer to the *Cisco IOS Security Configuration Guide*.

## RFC 1483 Encapsulation with NAT

This scenario shows a remote user connecting to the Internet through an ATM connection with RFC 1483 encapsulation and NAT. You may want to use this scenario if RFC 1483 connections can be used for the network because there is slightly less overhead with RFC 1483 encapsulation than with PPP.

Figure 4-12 and Table 4-14 show the network topology for this scenario.

***Figure 4-12 RFC 1483 Encapsulation with NAT***



| Callout Number | Description |
|---|---|
| **1** | Small business or remote user |
| **2** | Connection to Ethernet 0 address 192.168.1.1/24 |
| **3** | ATM 0 PVC 8/35 |
| **4** | The Internet |

In this scenario, the small business or remote user on the Ethernet LAN can connect to the Internet through ADSL. The Ethernet interface carries the data packet through the LAN and offloads it to the RFC 1483 connection on the ATM interface. The number of ATM PVCs is set by default.

NAT (represented as the dashed line at the edge of the 827 routers) signifies two addressing domains and the inside source address. The source list defines how the packet travels through the network.

The following configuration topics are covered in this section:

- Configuring the Ethernet Interface
- Configuring the ATM Interface
- Configuring NAT
- Configuration Examples

To add additional features to this network, see Chapter 7, "Router Feature Configuration."

After configuring your router, you need to configure the PVC endpoint. For a general configuration example, see the "Cisco 3640 Gateway Configuration Example" section on page 4-89.

## Configuring the Ethernet Interface

Complete the following steps to configure the Ethernet interface, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **interface ethernet 0** | Enter configuration mode for the Ethernet interface. |
| Step 2 | **ip address 192.168.1.1 255.255.255.0** | Set the IP address and subnet mask for the Ethernet interface. |
| Step 3 | **no shutdown** | Enable the Ethernet interface. |
| Step 4 | **exit** | Exit configuration mode for the Ethernet interface. |

## Configuring the ATM Interface

Use this table to configure the ATM interface, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **interface ATM 0** | Enter configuration mode for the ATM interface. |
| Step 2 | **ip address 200.200.100.1 255.255.255.0** | Set the IP address and subnet mask for the ATM interface. |
| Step 3 | **pvc 8/35** | Create an ATM PVC for each end node with which the router communicates. |
| Step 4 | **protocol ip 200.200.100.254 broadcast** | Set the protocol broadcast for the IP address. |
| Step 5 | **encapsulation** *type* | Specify the encapsulation type for the PVC to be AAL5SNAP or AAL5MUX IP. |
| Step 6 | **no shutdown** | Enable the ATM interface. |
| Step 7 | **exit** | Exit configuration mode for the ATM interface. |

## Configuring NAT

Complete the follow steps to configure NAT, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **ip nat inside source list 1 pool interface ATM0 overload** | Enable dynamic translation of addresses permitted by the access list to one of addresses specified in the ATM interface. |
| Step 2 | **ip route 0.0.0.0.0.0.0.0 atm0** | Set the IP route to point to the ATM interface as a default gateway. |
| Step 3 | **access-list 1 permit 192.168.1.0.0.0.0.255** | Define a standard access list permitting addresses that need translation. |
| Step 4 | **interface ethernet 0** | Enter configuration mode for the Ethernet interface. |
| Step 5 | **ip nat inside** | Establish the Ethernet interface as the inside interface. |
| Step 6 | **exit** | Exit configuration mode for the Ethernet interface. |
| Step 7 | **interface atm 0** | Enter configuration mode for the ATM interface. |
| Step 8 | **ip nat outside** | Establish the ATM interface as the outside interface. |
| Step 9 | **exit** | Exit configuration mode for the ATM interface. |

## Configuration Examples

In the following configuration examples, you do not have to enter the commands marked “default.” These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

The following example shows an RFC 1483 LLC/SNAP encapsulation over ATM.

```
!
interface Ethernet0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast (default)
ip nat inside
!
interface ATM0
```

```
ip address 200.200.100.1 255.255.255.0
no ip directed-broadcast (default)
ip nat outside
no atm ilmi-keepalive (default)
pvc 8/35
                    encapsulation aal5snap
    protocol ip 200.200.100.254 broadcast
!
bundle-enable
!
ip nat inside source list 1 interface ATM0 overload
ip classless (default)
ip route 0.0.0.0 0.0.0.0 200.200.100.254
!
access-list 1 permit 192.168.1.0 0.0.0.255
!
end
```

The following is an example for configuring RFC 1483 VC-MUX.

```
ip subnet-zero
!
interface Ethernet0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast (default)
ip nat inside
!
interface ATM0
ip address 200.200.100.1 255.255.255.0
no ip directed-broadcast (default)
ip nat outside
no atm ilmi-keepalive (default)
pvc 8/35
                    encapsulation aal5mux ip
            protocol ip 200.200.100.254 broadcast
!
bundle-enable
!
ip nat inside source list 1 interface ATM0 overload
ip classless (default)
ip route 0.0.0.0 0.0.0.0 200.200.100.254
!
access-list 1 permit 192.168.1.0 0.0.0.255
!
end
```

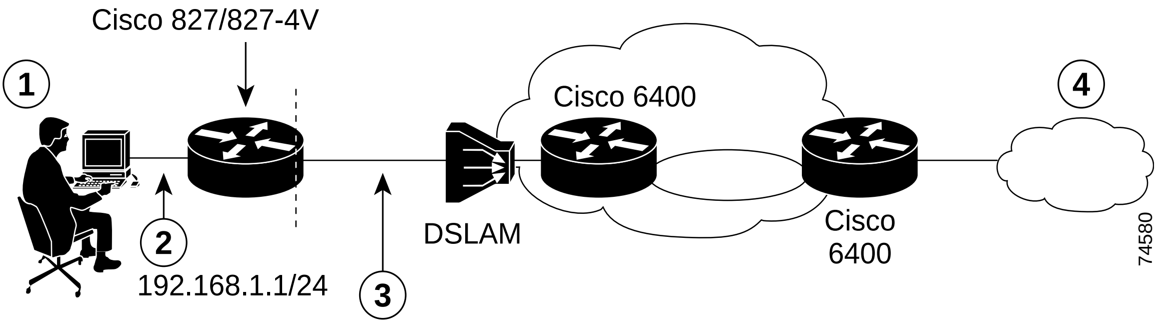
# Integrated Routing and Bridging

This network shows a user connecting to the Internet using integrated routing and bridging (IRB) to use NAT across a bridged interface. This scenario might work for you if you want to add functionality to an endpoint router without reconfiguring the central site. For example, you can provide an IP address and NAT in a bridged network without having to reconfigure the central site for routing.

Exchanging the bridge for a router enables the addition of features such as voice and quality of service (QoS). IRB provides more secure control of the central site and more efficient use of the WAN link.

Figure 4-13 and Table 4-15 show an IRB Internet scenario.

***Figure 4-13 IRB Internet Scenario***



| Callout Number | Description |
|---|---|
| **1** | Small business or remote user |
| **2** | Connection to Ethernet 0 address 192.168.1.1/24 |
| **3** | ATM 0 PVC 8/35 |
| **4** | The Internet |

One side of the network (the WAN, in this scenario) is configured to act as a bridge. The Bridge-Group Virtual Interface (BVI) is configured to act as a routed interface from the WAN bridge-group to the nonbridged LAN interface. From the LAN, the network appears as a router. From the WAN, the network appears as a bridge.

The ATM interface uses AAL5SNAP encapsulation. The number of PVCs is set by default.

NAT (represented as the dashed line at the edge of the Cisco 827 router) signifies two addressing domains and the inside source address. The source list defines how the packet travels through the network.

This section covers the following configuration topics:

- Configuring the Default Gateway
- Configuring the Ethernet Interface and IRB
- Configuring the ATM Interface
- Configuring the BVI
- Configuring NAT
- Configuration Example

To add more features to this network, see Chapter 7, "Router Feature Configuration."

After configuring your router, you need to configure the PVC endpoint. For a general configuration example, see the "Cisco 3640 Gateway Configuration Example" section on page 4-89.

## Configuring the Default Gateway

Enter the following command to set the IP route for the default gateway:

**ip route** *default-gateway ip address-mask*

## Configuring the Ethernet Interface and IRB

Complete the following steps to configure the Ethernet interface and IRB, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **bridge irb** | Specify IRB. |
| Step 2 | **bridge 1 route ip** | Enable IP routing to and from bridge-group 1. |
| Step 3 | **bridge 1 protocol ieee** | Specify the bridge protocol to define the type of Spanning-Tree Protocol (STP). |
| Step 4 | **interface ethernet 0** | Enter configuration mode for the Ethernet interface. |
| Step 5 | **ip address 192.168.1.1 255.255.255.0** | Set the IP address and subnet mask for the Ethernet interface. |
| Step 6 | **no shutdown** | Enable the Ethernet interface. |
| Step 7 | **exit** | Exit configuration mode for the Ethernet interface. |

## Configuring the ATM Interface

Follow the steps below to configure the ATM interface, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **interface ATM 0** | Enter configuration mode for the ATM interface. |
| Step 2 | **pvc 8/35** | Create an ATM PVC for each end node with which the router communicates. |
| Step 3 | **encapsulation aal5snap** | Specify the encapsulation type for the PVC. |
| Step 4 | **bridge-group 1** | Specify the bridge-group number to which the ATM interface belongs. |
| Step 5 | **no shutdown** | Enable the ATM interface. |
| Step 6 | **exit** | Exit configuration mode for the ATM interface. |

## Configuring the BVI

Follow the steps below to configure the BVI, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **interface bvi 1** | Enter configuration mode for the BVI. |
| Step 2 | **ip address 200.200.100.1 255.255.255.0** | Set the IP address and subnet mask for the BVI. |
| Step 3 | **exit** | Exit configuration mode for Ethernet interface. |

## Configuring NAT

Follow the steps below to configure NAT, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **ip nat pool test 200.200.100.1 200.200.100.1 255.255.255.0** | Create pool of global IP addresses for NAT. |
| Step 2 | **access-list 101 permit ip 192.168.1 0.0.0.0.255 any log** | Define a standard access list permitting addresses that need translation. |
| Step 3 | **ip nat inside source list 101 pool test overload** | Enable dynamic translation of addresses permitted by the access list to one of the addresses specified in the pool. |
| Step 4 | **interface ethernet 0** | Enter configuration mode for the Ethernet interface. |
| Step 5 | **ip nat inside** | Establish the Ethernet interface as the inside interface. |
| Step 6 | **no shutdown** | Enable interface and configuration changes just made to the interface. |
| Step 7 | **exit** | Exit configuration mode for the Ethernet interface. |

| | Command | Task |
|---|---|---|
| Step 8 | **interface ATM 0** | Enter configuration mode for the ATM interface. |
| Step 9 | **ip nat outside** | Establish the ATM interface as the outside interface. |
| Step 10 | **no shutdown** | Enable the interface and configuration changes just made to the interface. |
| Step 11 | **exit** | Exit configuration mode for the ATM interface. |
| Step 12 | **interface bvi 1** | Enter configuration mode for the BVI. |
| Step 13 | **ip nat outside** | Establish the BVI as the outside interface. |
| Step 14 | **no shutdown** | Enable the interface and configuration changes just made to the interface. |
| Step 15 | **end** | Exit configuration mode for the BVI. |

## Configuration Example

In the following configuration example, you do not have to enter the commands marked “default.” These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

```
bridge irb
!
interface Ethernet0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast (default)
ip nat inside
!
interface ATM0
no ip address
no ip directed-broadcast (default)
ip nat outside
no atm ilmi-keepalive (default)
pvc 8/35
encapsulation aal5snap
!
bridge-group 1
!
interface BVI1
ip address 200.200.100.1 255.255.255.0
```

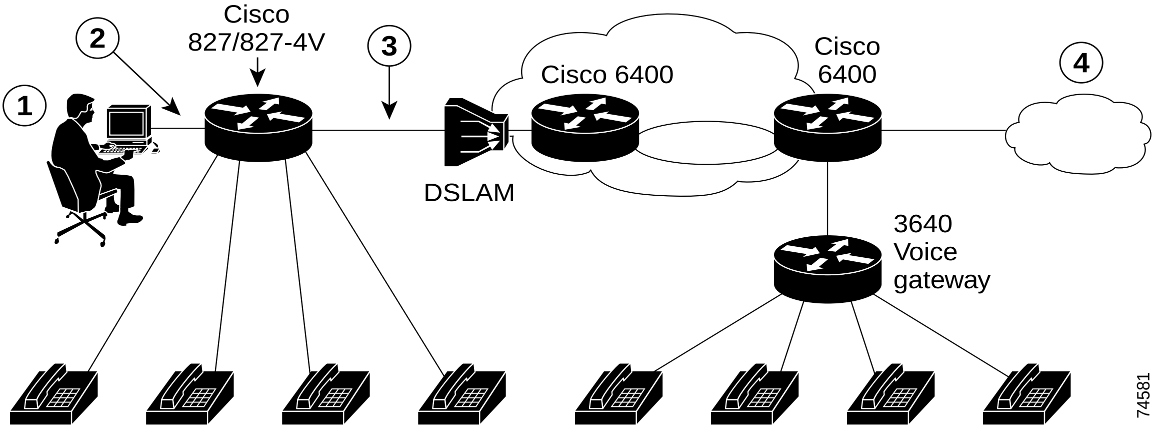
```
no ip directed-broadcast (default)
ip nat outside
!
ip nat pool test 200.200.100.1 200.200.100.1 netmask 255.255.255.0
ip nat inside source list 101 pool test overload
ip classless (default)
!
bridge 1 protocol ieee
bridge 1 route ip
!
access-list 101 permit ip 192.168.1.0 0.0.0.255 any log
!
ip route 0.0.0.0 0.0.0.0 200.200.100.254 (default gateway)
!
end
```

# Concurrent Routing and Bridging

This network shows a remote user connecting to the Internet using concurrent routing and bridging (CRB) to route voice traffic and bridge data traffic while keeping the two types of traffic separated. This scenario is useful if you want to simplify your network setup for data transmission and then configure voice. The IP address is configured to recognize the difference between data traffic and voice traffic (voice traffic is configured with QoS parameters and virtual circuits). IRB can do routing and bridging on the same interface; CRB does routing and bridging on separate interfaces.

Figure 4-14 and Table 4-16 show a CRB Internet scenario with the voice traffic routed and the data traffic bridged. Both the Cisco 827/827-4v gateway and the Cisco 3640 voice gateway are supporting voice traffic from telephones.

*Figure 4-14 CRB Internet Scenario*



| Callout Number | Description |
|---|---|
| **1** | Small business or remote user |
| **2** | Ethernet 0 bridge |
| **3** | ATM connection, ATM0.1 PVC 1/40 Voice 1.0.0.1/24, ATM0.2 PVC 8/35 data |
| **4** | The Internet |

Concurrent routing and bridging are accomplished using different subinterfaces under the ATM interface. Each ATM subinterface that is created is treated uniquely in the network.

Data traffic in this scenario is bridged across ATM subinterface 2, using AAL5SNAP encapsulation. A single PVC is created with a vpi/vci value of 8/35.

Voice traffic is routed across ATM0 subinterface 0.1. There is a single PVC created with a VPI/VCI value of 1/40 for voice. The voice subinterface is configured with remote dial peers to determine where outgoing calls are sent and with local dial peers to determine what numbers each port should respond to. Each VoIP dial peer is configured for H.323 signaling.

The following configuration topics are covered in this section:

- Specifying CRB and Configuring the Ethernet Interface
- Configuring the ATM Interface and Subinterfaces
- Configuring Voice Ports
- Configuring the POTS Dial Peers
- Configuring VoIP Dial Peers for H.323 Signaling
- Configuration Example

To add additional features to this network, see Chapter 7, "Router Feature Configuration."

After configuring your router, you need to configure the PVC endpoint. For a general configuration example, see the "Cisco 3640 Gateway Configuration Example" section on page 74.

## Specifying CRB and Configuring the Ethernet Interface

Follow the steps below to specify CRB and configure the Ethernet interface, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| **Step 1** | **bridge crb** | Specify CRB. |
| **Step 2** | **interface ethernet 0** | Enter configuration mode for the Ethernet interface. |
| **Step 3** | **bridge-group 1** | Specify the bridge-group number to which the Ethernet interface belongs. |
| **Step 4** | **exit** | Exit configuration mode for the Ethernet interface and the router. |
| **Step 5** | **bridge 1 protocol ieee** | Specify the bridge protocol to define the type of STP. |

## Configuring the ATM Interface and Subinterfaces

Follow the steps below to configure the ATM interface and subinterfaces, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| **Step 1** | **interface ATM 0.1 point-to-point** | Specify the ATM0.1 subinterface. |
| **Step 2** | **ip address 1.0.0.1 255.255.255.0** | Set the IP address and subnet mask for the ATM0.1 subinterface. |
| **Step 3** | **pvc 1/40** | Create an ATM PVC for each end node with which the router communicates. |
| **Step 4** | **encapsulation aal5snap** | Specify the encapsulation type for the PVC. |
| **Step 5** | **protocol ip 1.0.0.2 broadcast** | Set the protocol broadcast for the IP address. |
| **Step 6** | **interface ATM 0.2 point-to-point** | Specify the ATM0.2 subinterface. |
| **Step 7** | **pvc 8/35** | Create an ATM PVC for each end node with which the router communicates. |
| **Step 8** | **encapsulation aal5snap** | Specify the encapsulation type for the PVC. |
| **Step 9** | **bridge-group 1** | Specify the bridge-group number to which the Ethernet interface belongs. |
| **Step 10** | **no shutdown** | Enable the ATM interface. |
| **Step 11** | **exit** | Exit configuration mode for the ATM interface. |

## Configuring Voice Ports

To configure voice ports, you must configure the POTS dial peers and the VoIP dial peers for the signaling type; in this case, the type is H.323.

## Configuring the POTS Dial Peers

Complete the following steps to configure the POTS dial peers, beginning in global configuration mode. Table 4-3 shows the destination telephone number and port for each dial peer POTS port.

| | Command | Task |
|---|---|---|
| Step 1 | **dial-peer voice** *number* **POTS** | Enter configuration mode for the dial peer. |
| Step 2 | **destination-pattern** *string* | Define the telephone number associated with the port. |
| Step 3 | **voice port-number** | Specify the port number. |

*Table 4-3 Mapping of Dial Peer Number to Destination Telephone and Port*

| Dial Peer Number | Destination Pattern | Port |
|---|---|---|
| 101 | 14085271111 | 1 |
| 102 | 14085272222 | 2 |
| 103 | 14085273333 | 3 |
| 104 | 14085274444 | 4 |

## Configuring VoIP Dial Peers for H.323 Signaling

Follow the steps below to configure VoIP dial peers for H.323 signaling, beginning in global configuration mode. Table 4-4 shows the destination telephone number for each voice dial peer.

| | Command | Task |
|---|---|---|
| Step 1 | **dial-peer voice** *number* **VoIP** | Enter configuration mode for the dial peer. |
| Step 2 | **destination-pattern** *string* | Define the destination telephone number associated with each VoIP dial peer. |
| Step 3 | **codec g711ulaw** | Specify a codec if you are not using the default codec of g.729. |
| Step 4 | **session target ipv4:1.0.0.2** | Specify a destination IP address for each dial peer. |

*Table 4-4 Mapping of VoIP Dial Peers to Destination Telephone Numbers for H.323*

| VoIP Dial Peer | Destination Pattern |
|---|---|
| 1100 | 12123451111 |
| 1200 | 12123452222 |
| 1300 | 12123453333 |
| 1400 | 12123454444 |

## Configuration Example

In the following configuration example, you do not have to enter the commands marked “default.” These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

```
ip subnet-zero
!
bridge crb
!
interface Ethernet0
no ip address
no ip directed-broadcast (default)
bridge-group 1
!
interface ATM0
no ip address
no ip directed-broadcast (default)
no atm ilmi-keepalive (default)
bundle-enable
!
interface ATM0.1 point-to-point
ip address 1.0.0.1 255.255.255.0
no ip directed-broadcast (default)
pvc voice 1/40
protocol ip 1.0.0.2 broadcast
encapsulation aal5snap
!
interface ATM0.2 point-to-point
no ip address
no ip directed-broadcast (default)
pvc data 8/35
encapsulation aal5snap
!
```

```
bridge-group 1
!
ip classless (default)
!
bridge 1 protocol ieee
!
voice-port 1
local-alerting
!
voice-port 2
local-alerting
!
voice-port 3
local-alerting
!
voice-port 4
local-alerting
!
dial-peer voice 101 pots
destination-pattern 14085271111
port 1
!
dial-peer voice 1100 voip
destination-pattern 12123451111
codec g711ulaw
session target ipv4:1.0.0.2
!
dial-peer voice 102 pots
destination-pattern 14085272222
port 2
!
dial-peer voice 1200 voip
destination-pattern 12123452222
codec g711ulaw
session target ipv4:1.0.0.2
!
dial-peer voice 103 pots
destination-pattern 14085273333
port 3
!
dial-peer voice 1300 voip
destination-pattern 12123453333
codec g711ulaw
session target ipv4:1.0.0.2
!
dial-peer voice 104 pots
destination-pattern 14085274444
port 4
```

```
!
dial-peer voice 1400 voip
destination-pattern 12123454444
codec g711ulaw
session target ipv4:1.0.0.2
!
end
```

# Voice Scenario

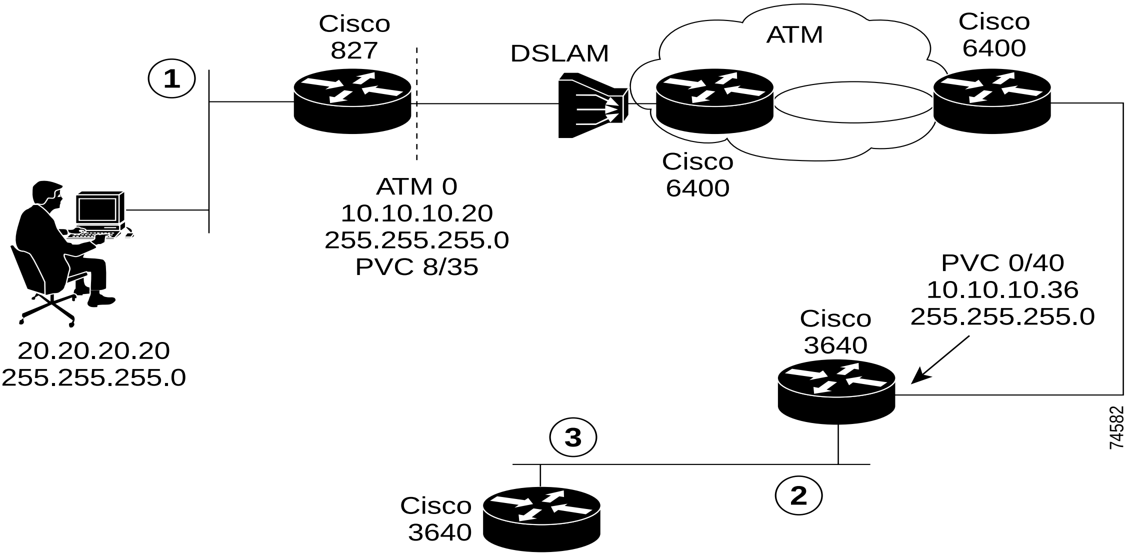
This section describes a voice scenario configuration using the Cisco 827 router in an H.323 signaling environment.

Setting up voice on the router actually includes two configurations—one for data and one for voice. When you have completed the configuration for the data scenario, you can add voice by configuring the POTS and VoIP dial peers and voice ports. Scenarios for data and voice are provided in the sections that follow.

## Data Network

Figure 4-15 and Table 4-19 show a data network with traffic routing through the Cisco 827 router and then switching on to the ATM interface.

*Figure 4-15 Data Network*



| Callout Number | Description |
|---|---|
| **1** | Ethernet connection to a Cisco 827 router |
| **2** | Ethernet connection 0/1 at address 172.17.1.1, subnet 255.255.255.0 |
| **3** | Ethernet connection 0 at 172.17.1.36, subnet 255.255.255.0 |

The Cisco 827 router is connected through the ATM interface through one PVC. The PVC is associated with a QoS policy called *mypolicy*. Data traffic coming from the Ethernet must have an IP precedence value of less than 5 (critical) to distinguish it from voice traffic.

EIGRP is configured to send 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, EIGRP assumes that the state of a destination has changed and sends an incremental update.

NAT (represented by the dashed line at the edge of the Cisco 827 router) signifies two addressing domains and the inside source address. The source list defines how the packet travels through the network.

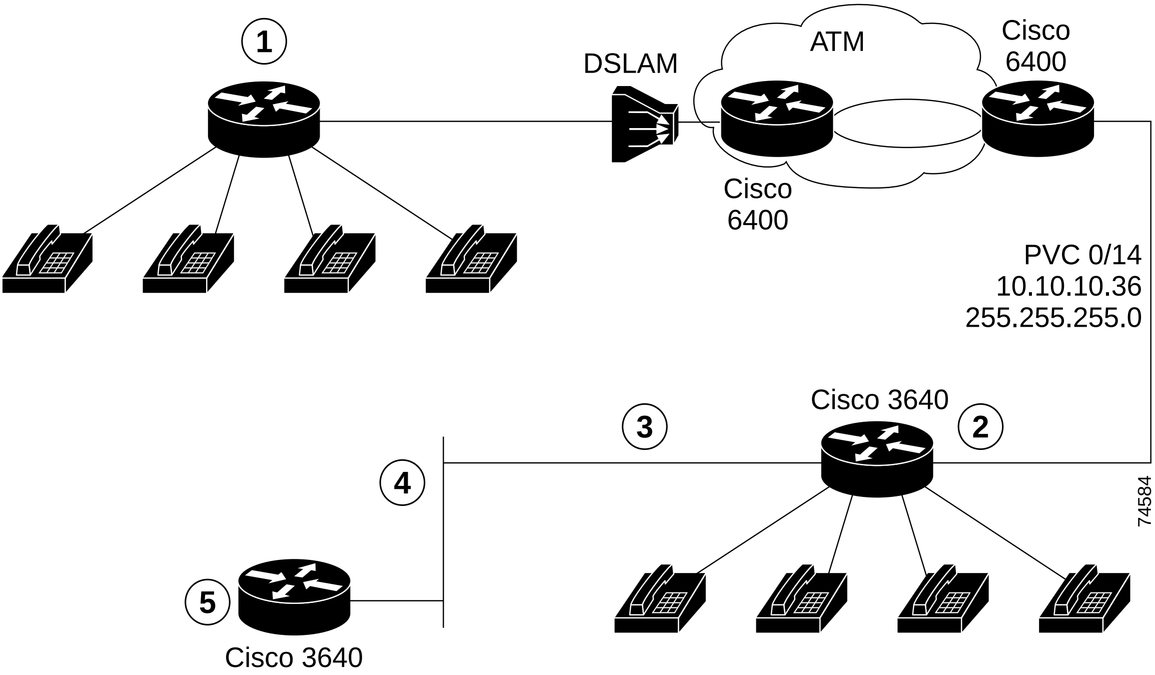
This scenario includes configuration tasks and a configuration example. To add more features to this network, see Chapter 7, "Router Feature Configuration."

After configuring your router, you need to configure the PVC endpoint. For a general configuration example, see the "Cisco 3640 Gateway Configuration Example" section on page 74.

# Voice Network

Figure 4-16 and Table 4-20 show a voice network with an 827-4V router and a Cisco 3640 router as the VoIP gateway using H.323 signaling (H.323 gateway).

*Figure 4-16 Voice Network*



| Callout Number | Description |
|---|---|
| **1** | Cisco 827-4V router serving as a voice gateway |
| **2** | Cisco 3640 router serving as a voice gateway |
| **3** | Ethernet 0 connection at address 172.17.1.36, subnet 255.255.255.0 |
| **4** | Ethernet 1 connection at address 172.17.1.1, subnet 255.255.255.0 |
| **5** | Cisco 3640 router serving as voice gatekeeper |

The Cisco 3640 router is set up on the LAN as a *gatekeeper*, which provides address translation and control access for the LAN for H.323 terminals and gateways. The gatekeeper may provide other services to the H.323 terminals and gateways, such as managing bandwidth and locating gateways.

In this scenario, the dial endpoint is the Cisco 3640 router, with an IP address of 172.17.1.36 and a subnet mask of 255.255.255.0. This configuration assumes a single-zone setup so that both the Cisco 827-4V router and the Cisco 3640 router are in the same zone.

Dialed numbers are stored by the VoIP session application in the 827-4V router, in this case, H.323. After enough digits are accumulated to match a configured destination pattern, the telephone number is mapped to a dial peer and session target. In this configuration, the dial peer has a session target of RAS, which is a protocol run between the H.323 session protocol gateway and gatekeeper.

The gatekeeper resolves the destination for each dialed number, and the call signal is routed to the Cisco 3640 gateway, which assigns the call to a voice port.

The coder-decoder compression schemes (codecs) are enabled for both ends of the connection, and QoS parameters are configured for IP precedence.

# Configuration Tasks

To configure the voice scenario, you must first configure the data network and then configure the voice network.

Configure the data network by following the procedures in these sections:

- Configuring the Class Map, Route Map, and Policy Map
- Configuring the Ethernet Interface
- Configuring the ATM Interface
- Configuring Enhanced IGRP

Then, configure the voice network by following the procedures in these sections:

- Configuring the POTS Dial Peers
- Configuring VoIP Dial Peers for H.323 Signaling

For configuration examples, see the "Configuring the Class Map, Route Map, and Policy Map" section on page 4-83, the "Configuring the Ethernet Interface" section on page 4-84, the "Configuring the ATM Interface" section on page 4-84, the "Configuring EIGRP" section on page 4-85, the "Configuring the POTS Dial Peers" section on page 4-86, and the "Configuring VoIP Dial Peers for H.323 Signaling" section on page 4-86 provided in the sections below.

Configuration examples are shown for the Cisco 827-4V router and the gateway and gatekeeper endpoint routers.

After configuring your router, you need to configure the PVC endpoint. For a general configuration example, see the "Cisco 3640 Gateway Configuration Example" section on page 74.

## Configuring the Class Map, Route Map, and Policy Map

Follow these steps to configure the class map, route map, and policy map, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **access-lists 101 permit ip any any precedence 5** | Configure the access list. |
| Step 2 | **class-map voice** | Configure the class map. |
| Step 3 | **match access-group 101** | Assign access list 101 to the class map. |
| Step 4 | **route-map data permit 10** | Configure the route map. |
| Step 5 | **ip precedence routine** | Set the IP precedence. |

| | Command | Task |
|---|---|---|
| Step 6 | **policy-map mypolicy** | Configure a policy map. |
| Step 7 | **class voice** | Specify the class for queuing voice traffic. |
| Step 8 | **priority 176** | Specify the bandwidth for queuing.[1] |
| Step 9 | **class class-default** | Configure the default class for all traffic but voice traffic. |

[1] Total bandwidth for the policy map may not exceed 75 percent of the total PVC bandwidth.

## Configuring the Ethernet Interface

Follow the steps below to configure the Ethernet interface, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **interface ethernet 0** | Enter configuration mode for the Ethernet interface. |
| Step 2 | **ip address 20.20.20.20 255.255.255.0** | Set the IP address and subnet mask for the Ethernet interface. |
| Step 3 | **ip policy route-map data** | Configure the IP policy route map. |
| Step 4 | **ip route-cache policy** | Enable fast-switching policy routing. |
| Step 5 | **no shutdown** | Enable the Ethernet interface. |
| Step 6 | **exit** | Exit configuration mode for the Ethernet interface. |

## Configuring the ATM Interface

Complete the following steps to configure the ATM interface, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **interface ATM 0** | Enter configuration mode for the ATM interface. |
| Step 2 | **ip address 10.10.10.20 255.255.255.0** | Set the IP address and subnet mask for the ATM interface. |
| Step 3 | **pvc 8/35** | Create an ATM PVC for each end node with which the router communicates. |
| Step 4 | **encapsulation aal5snap** | Specify the encapsulation type for the PVC. |
| Step 5 | **protocol ip 10.10.10.36 broadcast** | Specify the protocol broadcast for the IP address. |
| Step 6 | **service-policy output mypolicy** | Specify the service policy for the ATM interface. |
| Step 7 | **vbr-nrt 640 640 1** | Specify the ATM service class. |
| Step 8 | **no shutdown** | Enable the ATM interface. |
| Step 9 | **exit** | Exit configuration mode for the ATM interface. |

## Configuring EIGRP

Follow the steps below to configure EIGRP, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **router eigrp 100** | Enter router configuration mode, and enable EIGRP on the router. The autonomous-system number identifies the route to other EIGRP routers and is used to tag the EIGRP information. |
| Step 2 | **network** *number* | Specify the network number for each directly connected network. |
| Step 3 | **exit** | Exit router configuration mode. |

## Configuring the POTS Dial Peers

Follow the steps below to configure each POTS dial peer, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| **Step 1** | **dial-peer voice** *number* **POTS** | Enter configuration mode for the dial peer |
| **Step 2** | **destination-pattern** *string* | Define the destination telephone number associated with the VoIP dial peer. |
| **Step 3** | **port** *number* | Specify the port number. |

## Configuring VoIP Dial Peers for H.323 Signaling

Follow the steps below to configure VoIP dial peers for H.323 signaling in global configuration mode.

| | Command | Task |
|---|---|---|
| **Step 1** | **dial-peer voice** *number* **VoIP** | Enter configuration mode for the dial peer. |
| **Step 2** | **destination-pattern** *string* | Define the destination telephone number associated with each VoIP dial peer. |
| **Step 3** | **codec g711ulaw** | Specify a codec if you are not using the default codec of g.729. |
| **Step 4** | **ip precedence 5** | Set the IP precedence. |
| **Step 5** | **session target ras** | Specify a destination IP address for each dial peer. |

## Configuration Examples

This section contains the following configuration examples:

- Cisco 827-4V Router Configuration Example
- Cisco 3640 Gateway Configuration Example
- Cisco 3640 Gatekeeper Configuration Example

## Cisco 827-4V Router Configuration Example

The following is a configuration example for the Cisco 827-4V router portion of the voice network scenario. You do not have to enter the commands marked “default.” These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

```
!
class-map voice
match access-group 101
!
route-map data permit 10
set ip precedence routine
!
policy-map mypolicy
class voice
priority 176
class class-default
fair-queue 16 (default)
!
ip subnet-zero
!
gateway
!
interface Ethernet0
ip address 20.20.20.20 255.255.255.0
no ip directed-broadcast (default)
ip route-cache policy
ip policy route-map data
!
interface ATM0
ip address 10.10.10.20 255.255.255.0
no ip directed-broadcast (default)
no atm ilmi-keepalive (default)
pvc 1/40
service-policy output mypolicy
protocol ip 10.10.10.36 broadcast
vbr-nrt 640 640 1
! 640 is the maximum upstream rate of ADSL
encapsulation aal5snap
!
bundle-enable
h323-gateway voip interface
h323-gateway voip id gk-twister ipaddr 172.17.1.1 1719
h323-gateway voip h323-id gw-820
h323-gateway voip tech-prefix 1#
!
router eigrp 100
```

```
network 10.0.0.0
network 20.0.0.0
!
ip classless (default)
no ip http server
!
access-list 101 permit ip any any precedence critical(5)
!
line con 0
exec-timeout 0 0
transport input none
stopbits 1
line vty 0 4
login
!
!
voice-port 1
local-alerting
!
voice-port 2
local-alerting
!
voice-port 3
local-alerting
!
voice-port 4
local-alerting
!
dial-peer voice 10 voip
destination-pattern .......
ip precedence 5
session target ras
!
dial-peer voice 1 pots
destination-pattern 4085258111
port 1
!
dial-peer voice 2 pots
destination-pattern 14085258222
port 2
!
dial-peer voice 3 pots
destination-pattern 14085258333
port 3
!
dial-peer voice 4 pots
destination-pattern 14085258444
port 4
```

```
!
end
```

## Cisco 3640 Gateway Configuration Example

The following is a configuration example for the Cisco 3640 gateway portion of the voice network scenario. You do not have to enter the commands marked “default.” These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

```
!
class-map voice
match access-group 101
!
policy-map mypolicy
class voice
bandwidth 176
class class-default
fair-queue 16
!
ip subnet-zero
!
cns event-service server
!
voice-port 1/0/0
!
voice-port 1/0/1
!
voice-port 1/1/0
!
voice-port 1/1/1
!
dial-peer voice 10 voip
destination-pattern .......
ip precedence 5
session target ras
!
dial-peer voice 1 pots
destination-pattern 12125253111
port 1/0/0
!
dial-peer voice 2 pots
destination-pattern 12125253222
port 1/0/1
!
dial-peer voice 3 pots
```

```
destination-pattern 12125253333
port 1/1/0
!
dial-peer voice 4 pots
destination-pattern 12125253444
port 1/1/1
!
process-max-time 200
gateway
!
interface Ethernet0/0
ip address 172.17.1.36 255.255.255.0
no ip directed-broadcast
h323-gateway voip interface
h323-gateway voip id gk-twister ipaddr 172.17.1.1 1719
h323-gateway voip h323-id gw-3640
h323-gateway voip tech-prefix 1#
!
interface ATM2/0
ip address 10.10.10.36 255.255.255.0
no ip directed-broadcast
no atm ilmi-keepalive
pvc 8/35
service-policy output mypolicy
protocol ip 10.10.10.20 broadcast
vbr-rt 1000 600 1
encapsulation aal5snap
!
router eigrp 100
network 10.0.0.0
network 172.17.0.0
!
no ip classless
no ip http server
!
access-list 101 permit ip any any precedence critical (5)
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 0 4
login
!
!
end
```

## Cisco 3640 Gatekeeper Configuration Example

The following is a configuration example for the H.323 gatekeeper portion of the voice network scenario. You do not have to enter the commands marked “default.” These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

```
!
class-map voice
match access-group 101
!
!
policy-map mypolicy
class voice
bandwidth 176
class class-default
fair-queue 16
!
ip subnet-zero
!
ip dvmrp route-limit 20000
!
process-max-time 200
!
interface Ethernet0/0
ip address 172.28.9.83 255.255.255.0
no ip directed-broadcast (default)
!
interface Ethernet0/1
ip address 172.17.1.1 255.255.255.0
no ip directed-broadcast (default)
!
router eigrp 100
network 172.17.0.0
!
ip classless (default)
no ip http server
!
!
gatekeeper
zone local gk-router router.cisco.com 172.17.1.1
zone remote gk-sf1 cisco.com 179.15.2.2
zone remote gk-sf2 lucent.com 180.4.0.1
zone prefix gk-sf1 1415525....
zone prefix gk-sf2 1415527....
!
line con 0
exec-timeout 0 0
```

```
transport input none
line aux 0
line vty 0 4
password lab
login
!
end
```

CHAPTER 5

# Configuring Remote CAPI

## Overview of CAPI

The Common Application Programming Interface (CAPI) is an application programming interface standard used to access ISDN equipment connected to Basic Rate Interfaces (BRIs) and Primary Rate Interfaces (PRIs). Remote Common Application Programming Interface (RCAPI) is the CAPI feature configured remotely from a PC client. CAPI provides the following features:

- A standardized interface through which application programs use ISDN drivers and controllers. One application can use one or more controllers. Several applications can share one or more controllers.
- A selection mechanism that supports applications that use protocols at different levels and standardized network access. To provide this support, an abstraction from different protocol variables is performed by the software. All connection-related data, such as connection state and display messages, is available to the applications at any time.

The framing protocols supported by CAPI include High-Level Data Link Control (HDLC), HDLC inverted, bit transparent (speech), and V.110 synchronous/asynchronous. CAPI integrates the following data link and network layer protocols:

- Link Access Procedure on the D-channel (LAPD), in accordance with Q.921 for X.25 D-channel implementation
- Point-to-Point Protocol (PPP)
- ISO 8208 (X.25 DTE-DTE)
- X.25 DCE, T.90NL, and T.30 (fax Group 3)

# CAPI Features

CAPI supports the following features:

- Basic call features, such as call setup and tear-down
- Multiple B channels for data and voice connections
- Multiple logical data link connections within a physical connection
- Selection of different services and protocols during connection setup and on answering incoming calls
- Transparent interface for protocols above Layer 3
- One or more BRIs as well as PRI on one or more Integrated Services Digital Network (ISDN) adapters
- Multiple applications
- Operating-system-independent messages
- Operating-system-dependent exchange mechanism for optimum operating system integration
- Asynchronous event-driven mechanism, resulting in high throughput
- Well-defined mechanism for manufacturer-specific extensions
- Multiple supplementary services

# CAPI and RVS-COM

The router supports the ISDN Device Control Protocol (ISDN-DCP) from RVS-COM. ISDN-DCP allows a workstation on the LAN or router to use legacy dial computer telephony integration (CTI) applications. These applications include placing and receiving telephone calls and transmitting and receiving faxes.

Using ISDN-DCP, the router acts as a DCP server. By default, the router listens for DCP messages on TCP port number 2578 (the Internet-assigned number for RVS-COM DCP) on its LAN port.

When the router receives a DCP message from a DCP client (connected to the LAN port of the router), the router processes the message and acts on it. The router can send confirmations to the DCP clients and ISDN packets through the BRI port of the router.

When the router receives packets destined for one of the DCP clients on its BRI port, the router formats the packet as a DCP message and sends it to the corresponding client. The router supports all of the DCP messages in the ISDN-DCP specifications defined by RVS-COM.

# Supported B Channel Protocols

The router provides two 64-kbps B channels to CAPI clients. Each B channel can be configured separately to work in either HDLC mode or bit transparent mode. For CAPI support, layers B2 through B7 protocols are transparent to the applications using these B channels.

The ISDN core engine of RVS-COM supports the following B-channel protocols:

- CAPI layer B1
  - 64 kbps with HDLC framing
  - 64 kbps bit transparent operation with byte framing from the network
  - T.30 modem for fax Group 3
  - Modem with full negotiation
- CAPI layer B2
  - V.120
  - Transparent
  - T.30 modem for fax Group 3
  - Modem with full negotiation
- CAPI layer B3
  - Transparent
  - T.90NL with compatibility to T.70NL according to T.90 Appendix II
  - ISO 8208 (X.25 DTE-DTE) module 8 and windows size 2, no multiple logical connections
  - T.30 for fax Group 3
  - Modem with full negotiation

- T.30 for fax Group 3 (SFF file format [default], sending and receiving up to 14400 bits/sec with ECM option, modulations V.17, V.21, V.27ter, V.29)
- Analog modem (sending and receiving up to 14,400 bits/sec, modulations V.21, V.22, V.22bis, V.23, V.32, V.32bis)

# Supported D Channel Protocols

CAPI support is available only for the ISDN switch type Net3.

# Supported Applications

ISDN-DCP supports CAPI and non-CAPI applications. Applications are supported that use one or two B channels for data transfer, different HDLC-based protocols, Euro file transfer, or G4 fax; also supported are applications that send bit-transparent data such as A/Mu law audio, group 3 faxes, analog modem, or analog telephones.

# Requirements

Before you can enable the RCAPI feature on the Cisco 800 series router, the following requirements must be met:

- Cisco 800 series software with RCAPI support is installed on the router.
- CAPI commands are properly configured on the router.
- Both the CAPI local device console and RCAPI client devices on the LAN are correctly installed and configured with RVS-COM client driver software.

# Remote CAPI Default Setting

The default setting is disabled. To enable this feature, use the Cisco IOS **rcapi server port** command in global configuration mode:

**rcapi server port** *number*

**no rcapi server port**

where *number* is an optional parameter for the port number. If you do not enter a port number, the default port 2578 is used.

For more information, see the "Configuring Remote CAPI" chapter in the *Cisco 800 Series Software Configuration Guide.*

# Configuring RCAPI

The following procedure provides step-by-step instructions for configuring RCAPI on the Cisco 800 series router:

**Step 1** At the local device console, change to global configuration mode.

```
router# configure terminal
router(config)#
```

**Step 2** Set the switch type. In the following example, the switch type is set to European Telecommunication Standards Institute (ETSI).

```
router(config)# isdn switch-type basic-net3
```

**Step 3** Enter the RCAPI directory number assigned by the ISDN provider for the device. For example:

```
router(config)# rcapi number 12345
```

**Step 4** Optional. Perform this step only if you wish to specify a port number for RCAPI functions. Otherwise, the default port 2578 is used. Configure the same number on both the router and client PC. For example:

```
router(config)# rcapi server port 2000
```

**Step 5** Exit from global configuration mode to interface configuration mode.

```
router(config)# int bri0
```

**Step 6** Set the switch type for the BRI0 interface. In the following example, the switch type is set to ETSI.

```
router(config-if)# isdn switch-type basic-net3
```

**Step 7** Set the modem as the default handler for incoming voice calls.

```
router(config-if)# isdn incoming-voice modem
```

**Step 8** Change to privileged EXEC mode either by pressing **Ctrl-Z** or by entering **exit** twice, once at the interface mode prompt and again at the global configuration mode prompt.

```
router(config-if)# exit
router(config)# exit
router#
```

**Step 9** Optional. Enter the following if you wish to display RCAPI status.

```
router# show rcapi status
```

**Step 10** Optional. In privileged EXEC mode, start the debug program to run in the background.

```
router# debug rcapi events
```

**Step 11** If required, at each remote device console, change to global configuration mode. Repeat Step 2 through Step 10 to configure that device.

# Configuring Telephone Interfaces

The term *telephone port* refers to the physical port on the router back panel. The term *telephone interface* refers to a logical interface that you must configure to make an analog telephone or fax connected to a telephone port work properly.

This chapter describes how to configure standard and advanced features of the those Cisco 800 series routers supporting telephone features (Cisco 803, 804, and 813 routers). These routers support push-button analog telephones only; the Cisco routers do not support rotary telephones. This chapter also describes how to use the connected devices.

## Physical Characteristics

This section discusses the following:

- Physical characteristics that you must configure
- Tones that some users might need to configure
- Ringer equivalent number (REN)

### Configuring Physical Characteristics

Starting in global configuration mode, use these steps to configure physical characteristics. For information on the commands used in this table, refer to the Cisco IOS documentation set.

| | Command | Purpose |
|---|---|---|
| **Step 1** | **pots country** *country* | Enter the **pots country ?** command to get a list of supported countries and the code you must input to indicate a particular country. By specifying a country, you are configuring your telephone to use country-specific default settings for each physical characteristic. If you need to change a country-specific default setting, you can use the optional commands described in this table. |
| **Step 2** | **pots line-type** {**type1** \| **type2** \| **type3**} | Optional. Set the line type. Line type 1 runs at 600 ohms, line type 2 runs at 900 ohms, and line type 3 runs at 300 or 400 ohms. Lines in the U.S. typically run at 600 ohms (line type 1). |
| **Step 3** | **pots dialing-method** {**overlap** \| **enblock**} | Optional. Set the dialing method. If you select **overlap**, the router transmits each digit dialed in a separate message. If you select **enblock**, the router collects all digits dialed and transmits in one message. To interrupt collection and transmission of dial-string digits, enter pound sign (#) or stop dialing digits until a timer runs out. |
| **Step 4** | **pots disconnect-supervision** {**osi** \| **reversal**} | Optional. Set how the router notifies the connected device when calling party has hung up. Japan typically uses the **reversal** option. Most other countries use the **osi** option. |
| **Step 5** | **pots encoding** {**alaw** \| **ulaw**} | Optional. Set the pulse code modulation (PCM) encoding scheme. Europe typically uses the **alaw** option. North America typically uses the **ulaw** option. |

| | Command | Purpose |
|---|---|---|
| Step 6 | **pots tone-source** {**local** \| **remote**} | Optional. Set who supplies dial, ringback, and busy tones. If you select **local**, the router supplies the tones. If you select **remote**, the telephone switch provides the tones. For more information, refer to the "Tones for NET3 Switch" section on page 6-4. |
| Step 7 | **pots ringing-freq** {**20Hz** \| **25Hz** \| **50Hz**} | Optional. Set the frequency at which telephone ports ring. |
| Step 8 | **pots disconnect-time** *interval* | Optional. If a connected device, such as an answering machine, fails to detect that a calling party has hung up, you can adjust the interval at which selected disconnect supervision method is applied. Interval is from 50 to 2000 milliseconds. |
| Step 9 | **pots silence-time** *interval* | Optional. If a connected device, such as an answering machine, fails to detect that a calling party has hung up, you can adjust the interval of silence after a hang-up. Interval is from 0 to 10 seconds. |
| Step 10 | **pots distinctive-ring-guard-time** *milliseconds* | Optional. Set the delay, in milliseconds (0 to 1000), before a telephone port can be rung after a previous call is disconnected. For more information, refer to the "Distinctive Ringing" section on page 6-11. |
| Step 11 | **show pots status** | Optional. Display settings of physical characteristics as well as other information on telephone interfaces. |

## Tones for NET3 Switch

By default, the Cisco 800 series routers are configured so that the telephone switch supplies tones, such as dial, ringback, and busy tones. However, NET3 switches, which are used in Europe, do not provide these tones. You can use the **pots tone-source local** command from global configuration mode to configure the router instead of the telephone switch to provide these tones.

**Note** This command applies only to ISDN lines connected to a NET3 switch.

If the **pots dialing-method** command is set to enblock, the router provides the internal dial tone.

## REN

You can connect multiple devices (analog telephone or fax machine) to a router telephone port. The number of devices that you can connect depends on the following:

- REN of the telephone port (five).
- REN of each device that you plan to connect. (You can usually find the REN on the bottom of a device.)

If the REN of each device you plan to connect is one, then you can connect a maximum of five devices to that particular telephone port.

# Creating Dial Peers

You can create a dial peer to determine how incoming calls are routed to the telephone ports. You can create a total of six dial peers for the two telephone ports. There are no restrictions on how many dial peers you can create per port; for example, you can create six dial peers for port 1 and zero on port 2.

Starting from global configuration mode, use the steps below to create a dial peer.

| | Command | Purpose |
|---|---|---|
| **Step 1** | **dial-peer voice** *tag* **pots** | Set up tag number (1 through 6) for dial peer. |
| **Step 2** | **destination-pattern** *ldn* | Specify local ISDN directory number assigned to telephone interface. Do not specify an area code. |
| **Step 3** | **port** *port-number* | Specify number (1 or 2) associated with telephone port. |
| **Step 4** | **no call-waiting** | Optional. Disable call waiting. |
| **Step 5** | **ring** *cadence-number* | Optional. Set up distinctive ring (0 through 2). For more information, see the "Distinctive Ringing" section on page 6-11. |
| **Step 6** | **show dial-peer voice** [*tag*] | Optional. Display all or a particular dial-peer configuration (1 through 6). |

For example, if you have connected one voice device (555-1111) to port 1 and another (555-2222) to port 2, you can create two dial peers. The following output example shows two dial peers:

```
dial-peer voice 1 pots
destination-pattern 5551111
port 1
no call-waiting
ring 0
dial-peer voice 2 pots
destination-pattern 5552222
port 2
no call-waiting
ring 0
```

When a caller dials 555-1111, the call is routed to port 1. When a caller dials 555-2222, the call is routed to port 2. If the dial peers are not created, calls to both numbers are routed to port 1.

**Note** Make sure that all ISDN directory numbers associated with a service profile identifier (SPID) are associated with one port. For example, if both 555-1111 and 555-2222 are associated with SPID 1 and you associate 555-1111 to port 1 and 555-2222 to port 2, you will not be able to make calls on ports 1 and 2 simultaneously.

## What You Need to Know About SPIDs

North America uses SPIDs to identify subscribed services. The SPID format is generally an ISDN telephone number with several numbers added to it, such as 40855511110101. Your ISDN line could be assigned zero, one, or two SPIDs.

You must associate a SPID with an ISDN directory number and a telephone port number by using the **isdn spid1** and **isdn spid2** commands in global configuration mode and the **port** command in dial peer configuration mode. Make sure that you specify all the ISDN directory numbers provided by your telephone service provider in the **isdn spid1** and **isdn spid2** commands. Also make sure that all ISDN directory numbers associated with a SPID are associated with the same telephone port. For information on using the **port** command while setting up a dial peer, see the "Creating Dial Peers" section on page 6-4.

## Forwarding Incoming ISDN Voice Calls to Connected Devices

Starting from global configuration mode, follow these steps:

| | Command | Purpose |
|---|---|---|
| **Step 1** | **interface bri0** | Specify parameters for the WAN interface. |
| **Step 2** | **isdn incoming-voice modem** | Specify that incoming ISDN voice calls are forwarded to devices connected to telephone ports. |

Note If you do not enter the **isdn incoming-voice modem** command, the router rejects incoming ISDN voice calls.

# Configuring Advanced Telephone Features

This section describes advanced telephone features and how to configure them.

## ISDN Voice Priority

The ISDN voice priority feature controls the priority of data and voice calls for telephones or fax machines connected to the router telephone ports. If an ISDN circuit endpoint is busy with a data call or calls and either a voice call comes in (incoming) or you attempt to place a voice call (outgoing), the data call is handled per the voice priority setting.

You can configure the router so that data calls are handled in one of the following ways:

- A voice call always supercedes ("bumps") a data call. This is the default setting.
- A voice call supercedes a data call only if there are more than one call to the same destination.
- A voice call never supercedes a data call.

Use the following command to reconfigure the priority.

| Command | Purpose |
|---|---|
| **isdn voice-priority** *local-directory-number* {**in** \| **out**} {**always** \| **conditional** \| **off**} | Configure ISDN voice priority for each ISDN directory number. |

If you have multiple ISDN directory numbers associated with a SPID, then the outgoing voice priority that you set for any of these directory numbers applies to the other numbers.

For example, if you enter the following command, the outgoing voice priority for all directory numbers specified in the **isdn spid1** command is set to conditional:

```
router(config-if)# isdn spid1 0 4085551111 4085552222 4085553333
router(config-if)# isdn voice-priority 5551111 out conditional
```

Table 6-1 describes the possible data call scenarios, what happens when a voice call comes in, and what happens when you place an outgoing voice call with a particular configuration.

*Table 6-1 Incoming and Outgoing ISDN Voice Priority Scenarios*

| Scenario | Always | Conditional | Off |
|---|---|---|---|
| Two data channels to destination A. | Bump one data channel when you pick up handset to answer incoming voice call or to place outgoing voice call. | Bump one data channel when you pick up handset to answer incoming voice call or to place outgoing voice call. | No bump; voice caller receives busy signal. |
| One data channel to destination A;<br>one data channel to destination B. | Bump one data channel when you pick up handset to answer incoming voice call or to place outgoing voice call. | No bump; voice caller receives busy signal. | No bump; voice caller receives busy signal. |

The setting of the **pots dialing-method** command determines whether you hear a busy signal if a data call cannot be bumped when you are trying to make an outgoing call. If the setting is **overlap**, you hear a busy signal when you pick up the handset. If the setting is **enblock**, you hear a dial tone initially, then a busy signal.

# Data over Voice Bearer Service

**Note** This section applies only to analog telephone services in the U.S.

In some tariff areas, voice calls are less expensive than data calls. If this is the case in your tariff area, the Cisco 800 series routers support incoming and outgoing data over voice (DOV) calls. DOV calls are data calls made over the ISDN line using voice bearer capability (VBC).

The router recognizes the difference between a data call and a voice call. Incoming data calls are routed to the LAN over the Ethernet port. If a telephone interface has been configured for DOV, incoming data calls made with VBC are routed to the LAN over the Ethernet port. Figure 6-1 and Table 6-2 illustrate a data call being routed to the LAN.

Incoming voice calls are forwarded to the analog device over the analog telephone port, as shown in Figure 6-2 and Table 6-3.

***Figure 6-1 Data Call over VBC Line***

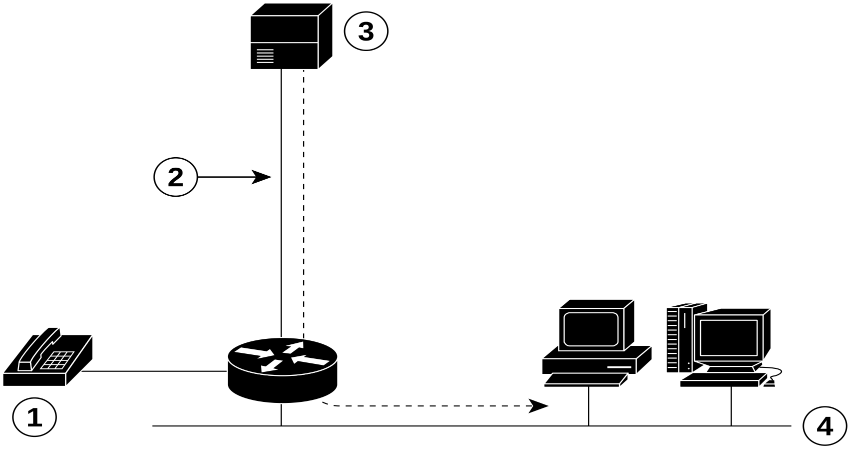


Table 6-2 Key for Data Call over VBC Line

| Callout Number | Description |
|---|---|
| 1 | Analog telephone |
| 2 | ISDN BRI line with VBC |
| 3 | Central office switch |
| 4 | Ethernet LAN |

Figure 6-2 Voice Call over VBC Line

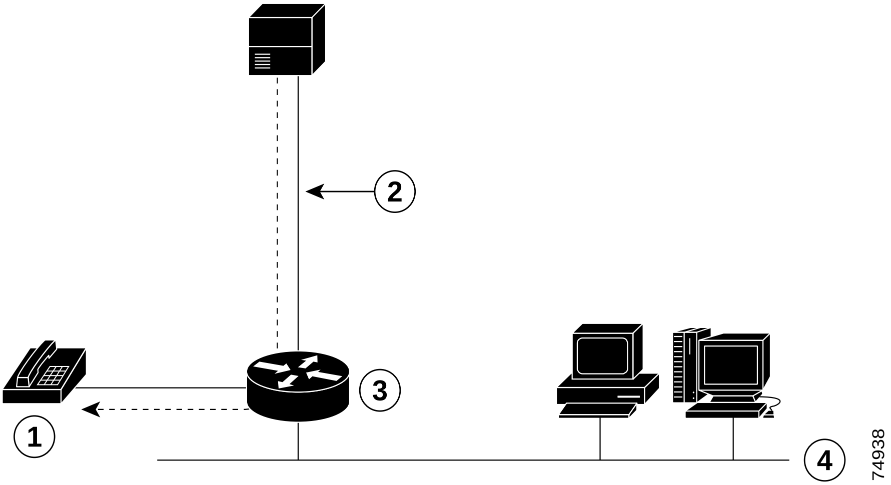


Table 6-3 Key for Voice Call over VBC Line

| Callout Number | Description |
|---|---|
| 1 | Analog telephone |
| 2 | ISDN BRI line with VBC |
| 3 | Router |
| 4 | Ethernet LAN |

**Note** When the router is configured for DOV, ISDN BRI calls are made with VBC, which has a data rate of 56 kbps, instead of the usual ISDN BRI data rate of 64 kbps.

Use the following command to configure the router to accept incoming DOV calls:

**isdn incoming-voice data 56**

Follow these steps to configure the router to place outgoing DOV calls:

| | Command | Purpose |
|---|---|---|
| **Step 1** | **class voice** *number* | Create a dialer map. |
| **Step 2** | **map-class dialer voice** | Define a class of shared configuration parameters for outgoing calls. |
| **Step 3** | **dialer voice-call** | Configure router to make outgoing DOV calls. |
| **Step 4** | **dialer isdn speed 56** | Specify bit rate used on B channel associated with specified map class. |

# Distinctive Ringing

A *ringing cadence* is a pattern of a ringing and a quiet period. There are two types of ringing cadences: a primary ringing cadence and distinct ringing. The primary cadence is determined by the country where your router is located. In addition to the primary cadence, you can configure up to two distinctive rings on a telephone port.

Because the router associates a distinctive ring with the ISDN directory number assigned to an interface, you must configure a distinctive ring with a dial peer. For information on dial peers and how to configure them, see the "Creating Dial Peers" section on page 6-4.

**Note** Generally your telephone service provider assigns one ISDN directory number for each SPID. You must have one ISDN directory number for each distinctive ring that you set up. Therefore, if you want to set up two distinctive rings, you must request an additional ISDN directory number from your telephone service provider.

To configure the ringing cadence, insert the following commands into a dial-peer configuration:

**ring** *cadence-number*

where *cadence-number* can be 0, 1, or 2.

- Type 0 is a primary ringing cadence—default ringing cadence for country your router is located in.
- Type 1 is a distinctive ring—0.8 seconds on, 0.4 seconds off, 0.8 seconds on, 4 seconds off.
- Type 2 is a distinctive ring—0.4 seconds on, 0.2 seconds off, 0.4 seconds on, 0.2 seconds off, 0.8 seconds on, 4 seconds off.

By default, the ring cadence is set to 0, which means that the interface uses the primary ringing cadence.

You can also insert the following command syntax into a dial-peer configuration:

**pots distinctive-ring-guard-time** *milliseconds*

where *milliseconds* can be a number from 50 to 1000. This command configures the delay, in milliseconds, before a telephone port can be rung after a previous call is disconnected. The default is no delay.

# Caller Identification

In addition to an analog telephone or fax machine, North American users can connect a caller ID device to the router telephone ports. This device displays the telephone numbers of incoming callers. The Cisco 800 series routers support the following caller ID devices:

- AT&T 25
- AT&T 85 Plus

- CIDCO
- Fans Callscreener
- GE Caller ID with phone
- GE Caller ID without phone
- Northwestern Bell Phone, Bell Phone
- Radio Shack Caller ID System 350

The Cisco 800 series routers do not support the following devices:

- Southwestern Bell Freedom Phone
- TTY System

# How to Use Telephones Connected to Cisco 800 Series Routers

This section describes how to make a basic call and how to use the supplementary services that you ordered from your telephone service provider.

## Making a Basic Call

To make a basic telephone call, pick up the handset, and dial the number of the desired party.

To make a basic call if your router is connected to a Nippon Telegraph and Telephone (NTT) switch, follow these steps:

**Step 1** Dial the telephone number.

You must enter each digit within 12 seconds of entering the previous digit. If you wait longer than 12 seconds, an incomplete set of digits is sent to the switch.

**Step 2** Send the entire set of digits to the switch by using one of the following methods:

- Press the pound key (#) on the telephone keypad.
- Wait 12 seconds without entering any digits. After 12 seconds, the router sends the set of digits to the switch.

## Disabling Pound Key End-of-Call Function

You can disable the end-of-call function (initiated by pressing the pound key [#]) by entering the following command on the telephone keypad:

****98#**

**Note** This command applies only to ISDN lines connected to an NTT switch.

You can disable this function if a telephone number you are dialing requires the pound key (#) as one of the digits. After entering the ****98#** command, wait for a dial tone and then enter the digits, including the pound key. To send the digits to the switch, wait 6 seconds without entering any digits.

The end-of-call function automatically resumes for the next call.

# Using Supplementary Services

This section describes how to use the following supplementary services:

- Call Holding and Retrieving
- Call Waiting
- Three-Way Conference Call
- Call Transfer
- Call Forwarding

## Call Holding and Retrieving

For this feature to work, you must request it when you order your ISDN line. For information on ordering your ISDN line, see Appendix D, "Provisioning an ISDN Line." However, you do not need to configure the router to make this feature work.

You can put an active voice call on hold, make a second call, and toggle between the two calls. Follow these steps:

**Step 1** Put the active call on hold, and get a dial tone by quickly pressing the telephone receiver (flash) button once, and then entering ****95#** on the telephone keypad.

**Step 2** Make the second call.

**Step 3** Toggle between the two calls by quickly pressing the flash button.

If you hang up with a call still on hold, the phone rings to remind you of the outstanding call. Pick up the handset to reconnect to the call.

## Call Waiting

For this feature to work, you must request it when you order your ISDN line. For information on ordering your ISDN line, see Appendix D, "Provisioning an ISDN Line."

By default, call waiting is enabled. You can disable it permanently by using the **no call-waiting** command. (You might want to disable it for fax machines.) Because the router associates call waiting with the ISDN directory number assigned to a telephone interface, you should disable call waiting at the same time that you are configuring a dial peer. For information on dial peers and how to configure them, refer to the "Creating Dial Peers" section on page 6-4.

To disable call waiting on a per-call basis, enter ****99#** on the telephone keypad.

During an active voice call, a call-waiting tone sounds if another call comes in. Subsequent tones sound at 10-second intervals until the incoming caller hangs up or until you answer the call. During this time, the incoming caller hears ringing.

When you hear the call-waiting tone, you can do one of the following:

- Put the current call on hold, and answer the incoming call
- Hang up the current call, and answer the new call.

To put the current call on hold and answer the incoming call, quickly press the telephone receiver (flash) button once. Press this button again to go back to the current call.

## Three-Way Conference Call

For this feature to work, you must request it when you order your ISDN line. For information on ordering your ISDN line, see Appendix D, "Provisioning an ISDN Line."

If you are connected to a National ISDN-1 (NI1) or a Northern Telecom DMS-100 custom switch, you might need to activate this feature by using the following command syntax:

**isdn conference-code** *range*

The range is from 0 to 999. The default code is 60. Your telephone service provider should provide a code when you order this feature; if a code other than 60 is provided, you need to reconfigure the code using the **isdn conference-code** command.

Otherwise, you do not need to configure the router to make this feature work.

You can talk simultaneously with two other parties. To create a conference call, follow these steps:

**Step 1** Put the first party on hold and get a dial tone by quickly pressing the telephone receiver (flash) button once.

**Step 2** Dial the second party.

**Step 3** Add the first party to the call by quickly pressing the flash button.

## Call Transfer

For this feature to work, you must request it when you order your ISDN line. For information on ordering your ISDN line, see Appendix D, "Provisioning an ISDN Line."

If you are connected to a National ISDN-1 (NI1) or a Northern Telecom DMS-100 Custom switch, you might need to activate this feature, using the following command syntax:

**isdn transfer-code** *range*

The range is from 0 to 999. The default code is 61. Your telephone service provider should provide a code when you order this feature; if a code other than 61 is provided, you need to reconfigure the code by using the **isdn transfer-code** command.

Otherwise, you do not need to configure the router to make this feature work.

You can transfer an incoming or outgoing voice call to another party. To transfer a call, do the following:

**Note** If you are connected to an NTT switch, you will not be able to transfer an outgoing call.

**Step 1** Put the first party on hold, and get a dial tone by quickly pressing the telephone receiver (flash) button once.

**Step 2** Dial the second party to which you want to transfer the call.

**Step 3** While still connected to the second party, hang up.

Hanging up connects the first and second parties. Instead of doing Step 3, you can also create a three-way call conference by quickly pressing the flash button once.

If the call to the second party fails, you can return to the first party by doing one of the following:

- Quickly pressing the telephone receiver (flash) button once
- Hanging up

If you hang up, the telephone rings to indicate that the first party is still on hold.

## Call Forwarding

The call forwarding feature works for Sweden and Finland only. For this feature to work, you must request it when you order your ISDN line. For information on ordering your ISDN line, see Appendix D, “Provisioning an ISDN Line.”

The router supports the following call forwarding features:

- Call forwarding unconditional (CFU)—you can forward all incoming calls to another telephone number.
- Call forwarding no reply (CFNR)—you can forward incoming calls that are not answered within a defined period to another telephone number.
- Call forwarding busy (CFB)—you can forward incoming calls that get a busy signal to another telephone number.

To make sure that the router accepts the activation and deactivation of the call forwarding features using the telephone keypad, use the **pots country** *country* command in global configuration mode. The *country* variable is the country that your router is in. Enter the **pots country ?** command to get a list of supported countries and the code you must enter to indicate a particular country.

To activate call forwarding unconditional, call forwarding no reply, or call forwarding busy, follow these steps:

**Step 1** Pick up the telephone handset.

**Step 2** Enter the following on the telephone keypad:

**feature-number* **telephone-number-to-forward-to*#

Your telephone service provider should provide the number for each call forwarding feature. For example, to forward a call to 408-555-2222, enter the following:

```
*21*4085552222#
```

**Step 3** Hang up the handset.

To deactivate call forwarding unconditional, call forwarding no reply, or call forwarding busy, follow these steps:

**Step 1** Pick up the telephone handset.

**Step 2** Enter the following on the telephone keypad:

#*feature-number*#

Your telephone service provider should provide the number for each call forwarding feature. For example, to deactivate call forwarding, enter the following:

**#21#**

**Step 3** Hang up the handset.

**Note** In the U.S., the call forwarding variable (CFV) feature is available with the NI1 capability package EZ-1. With CFV, you can forward incoming calls. You can turn this feature on or off through access codes supplied by your telephone service provider.

# POTS Dial Feature (Japan Only)

The Cisco 813 router supports the plain old telephone service (POTS) dial feature for Japanese telephones. This feature can be activated by a dial application on your workstation that dials a telephone number for the POTS port on the Cisco 813 router. The telephone connected to the port can be on- or off-hook when the dial command is issued. If the telephone is on-hook, the router rings the telephone, waits until the telephone is taken off hook, then dials the number requested. If the telephone is off-hook when the command is issued, the router dials the number requested, provided that the telephone is receiving a dial tone.

## Activating the POTS Dial Feature

Each time you wish to activate this feature on the router for use by the dial application, enter the following Cisco IOS command in EXEC mode:

```
test pots port dial number [#]
```

where *port* is the port number 1 or 2, and *number* is the telephone number to dial.

**Note** The router does not turn off dual tone multifrequency (DTMF) detection from the telephone when you enter the POTS dial command. If you do not terminate the *number* variable with a pound (**#)** character, you can complete the call by using the telephone key pad.

The following example shows the POTS dial command:

```
router# test pots 1 dial 4085551234#
```

## Displaying POTS Call State

To show the current state of POTS calls and the most recent event received by the call switching module (CSM), use the **show pots csm** command in EXEC mode.

```
show pots csm port
```

where *port* is port number 1 or 2.

### Output Example

The following is an example of the **show pots csm** command screen output:

```
router# show pots csm 1

POTS PORT: 1

   CSM Finite State Machine:
      Call 0 - State: idle, Call Id: 0x0
               Active: no
               Event: CSM_EVENT_NONE Cause: 0
      Call 1 - State: idle, Call Id: 0x0
               Active: no
               Event: CSM_EVENT_NONE Cause: 0
      Call 2 - State: idle, Call Id: 0x0
               Active: no
               Event: CSM_EVENT_NONE Cause: 0

router#
```

## Disconnecting a POTS Call

To disconnect a telephone call for the POTS port on the router, use the **test pots** *port* **disconnect** command in EXEC mode:

**test pots** *port* **disconnect**

where *port* is the port number 1 or 2.

The following example disconnects a telephone call from POTS port 1:

```
router# test pots 1 disconnect
router#
```

## POTS Debug Command

To display the status of calls made to and from the POTS ports, enter the following command in EXEC mode:

```
debug pots csm
```

Entering this command activates events by which your dial application can determine the progress of calls to and from the ports.

## Debug Message Formats

Debug messages are displayed in one of two formats that are relevant to the POTS dial feature:

```
hh:mm:ss: CSM_STATE: CSM_EVENT, call id = ??, port = ?
```

or

```
hh:mm:ss: EVENT_FROM_ISDN:dchan_idb=0x???????, call_id=0x????, ces=?
bchan=0x????????, event=0x?, cause=0x??
```

where:

- *hh:mm:ss* is a timestamp in hours, minutes, and seconds.
- *CSM_STATE* is one of the call switching module (CSM) states listed in Table 6-4.
- *call id* is a hexadecimal value from 0x00 to 0xFF.
- *port* is telephone port 1 or 2.
- *EVENT_FROM_ISDN* is a CSM event. Table 6-5 shows a list of CSM events.
- *dchan_idb* is an internal data structure address.
- *ces* is the connection end point suffix used by ISDN.
- *bchan* is the channel used by the call. A value of 0xFFFFFFFF indicates that a channel is not assigned.
- *event* is represented by a hexadecimal value that is translated into a CSM event. Table 6-6 shows a list of events and the corresponding CSM events.
- *cause* is represented by a hexadecimal value that is given to call-progressing events. Table 6-7 shows a list of cause values and definitions.

## CSM States

Table 6-4 shows the values for CSM states.

***Table 6-4 CSM States***

| CSM State | Description |
|---|---|
| CSM_IDLE_STATE | Telephone on hook |
| CSM_RINGING | Telephone ringing |

*Table 6-4 CSM States (continued)*

| CSM State | Description |
|---|---|
| CSM_SETUP | Setup for outgoing call in progress |
| CSM_DIALING | Dialing number of outgoing call |
| CSM_IVR_DIALING | Interactive voice response (IVR) for Japanese telephone dialing |
| CSM_CONNECTING | Waiting for carrier to connect the call |
| CSM_CONNECTED | Call connected |
| CSM_DISCONNECTING | Waiting for carrier to disconnect the call |
| CSM_NEAR_END_DISCONNECTING | Waiting for carrier to disconnect the call |
| CSM_HARD_HOLD | Call on hard hold |
| CSM_CONSULTATION_HOLD | Call on consultation hold |
| CSM_WAIT_FOR_HOLD | Waiting for carrier to put call on hard hold |
| CSM_WAIT_FOR_CONSULTATION_HOLD | Waiting for carrier to put call on consultation hold |
| CSM_CONFERENCE | Waiting for carrier to complete call conference |
| CSM_TRANSFER | Waiting for carrier to transfer call |
| CSM_APPLIC_DIALING | Call initiated from Cisco IOS command-line interface (CLI) |

## CSM Events

Table 6-5 shows the values for CSM events.

*Table 6-5 CSM Events*

| CSM Events | Description |
|---|---|
| CSM_EVENT_INTER_DIGIT_TIMEOUT | Time waiting for dial digits has expired |
| CSM_EVENT_TIMEOUT | Near or far end disconnect timeout |
| CSM_EVENT_ISDN_CALL | Incoming call |
| CSM_EVENT_ISDN_CONNECTED | Call connected |
| CSM_EVENT_ISDN_DISCONNECT | Far end disconnected |

*Table 6-5 CSM Events (continued)*

| CSM Events | Description |
|---|---|
| CSM_EVENT_ISDN_DISCONNECTED | Call disconnected |
| CSM_EVENT_ISDN_SETUP | Outgoing call requested |
| CSM_EVENT_ISDN_SETUP_ACK | Outgoing call accepted |
| CSM_EVENT_ISDN_PROC | Call proceeding and dialing completed |
| CSM_EVENT_ISDN_CALL_PROGRESSING | Call being received in band tone |
| CSM_EVENT_ISDN_HARD_HOLD | Call on hard hold |
| CSM_EVENT_ISDN_HARD_HOLD_REJ | Hold attempt rejected |
| CSM_EVENT_ISDN_CHOLD | Call on consultation hold |
| CSM_EVENT_ISDN_CHOLD_REJ | Consultation hold attempt rejected |
| CSM_EVENT_ISDN_RETRIEVED | Call retrieved |
| CSM_EVENT_ISDN_RETRIEVE_REJ | Call retrieval attempt rejected |
| CSM_EVENT_ISDN_TRANSFERRED | Call transferred |
| CSM_EVENT_ISDN_TRANSFER_REJ | Call transfer attempt rejected |
| CSM_EVENT_ISDN_CONFERENCE | Call conference started |
| CSM_EVENT_ISDN_CONFERENCE_REJ | Call conference attempt rejected |
| CSM_EVENT_ISDN_IF_DOWN | ISDN interface down |
| CSM_EVENT_ISDN_INFORMATION | ISDN information element received (used by Nippon Telegraph and Telephone [NTT] IVR application) |
| CSM_EVENT_VDEV_OFFHOOK | Telephone off hook |
| CSM_EVENT_VDEV_ONHOOK | Telephone on hook |
| CSM_EVENT_VDEV_FLASHHOOK | Telephone hook switch has flashed |
| CSM_EVENT_VDEV_DIGIT | DTMF digit has been detected |
| CSM_EVENT_VDEV_APPLICATION_CALL | Call initiated from Cisco IOS command-line interface (CLI) |

## Events

Table 6-6 shows the values for events that are translated into CSM events.

*Table 6-6 Event Values and Corresponding CSM Events*

| Hexadecimal Value | Event | CSM Event |
|---|---|---|
| 0x0 | DEV_IDLE | CSM_EVENT_ISDN_DISCONNECTED |
| 0x1 | DEV_INCALL | CSM_EVENT_ISDN_CALL |
| 0x2 | DEV_SETUP_ACK | CSM_EVENT_ISDN_SETUP_ACK |
| 0x3 | DEV_CALL_PROC | CSM_EVENT_ISDN_PROC |
| 0x4 | DEV_CONNECTED | CSM_EVENT_ISDN_CONNECTED |
| 0x5 | DEV_CALL_PROGRESSING | CSM_EVENT_ISDN_CALL_PROGRESSING |
| 0x6 | DEV_HOLD_ACK | CSM_EVENT_ISDN_HARD_HOLD |
| 0x7 | DEV_HOLD_REJECT | CSM_EVENT_ISDN_HARD_HOLD_REJ |
| 0x8 | DEV_CHOLD_ACK | CSM_EVENT_ISDN_CHOLD |
| 0x9 | DEV_CHOLD_REJECT | CSM_EVENT_ISDN_CHOLD_REJ |
| 0xa | DEV_RETRIEVE_ACK | CSM_EVENT_ISDN_RETRIEVED |
| 0xb | DEV_RETRIEVE_REJECT | CSM_EVENT_ISDN_RETRIEVE_REJ |
| 0xc | DEV_CONFR_ACK | CSM_EVENT_ISDN_CONFERENCE |
| 0xd | DEV_CONFR_REJECT | CSM_EVENT_ISDN_CONFERENCE_REJ |
| 0xe | DEV_TRANS_ACK | CSM_EVENT_ISDN_TRANSFERRED |
| 0xf | DEV_TRANS_REJECT | CSM_EVENT_ISDN_TRANSFER_REJ |

## Cause Values

Table 6-7 shows cause values that are assigned only to call-progressing events.

*Table 6-7 Cause Values and Definitions*

| Hexadecimal Value | Cause Definitions |
|---|---|
| 0x01 | UNASSIGNED_NUMBER |
| 0x02 | NO_ROUTE |
| 0x03 | NO_ROUTE_DEST |
| 0x04 | NO_PREFIX |
| 0x06 | CHANNEL_UNACCEPTABLE |
| 0x07 | CALL_AWARDED |
| 0x08 | CALL_PROC_OR_ERROR |
| 0x09 | PREFIX_DIALED_ERROR |
| 0x0a | PREFIX_NOT_DIALED |
| 0x0b | EXCESSIVE_DIGITS |
| 0x0d | SERVICE_DENIED |
| 0x10 | NORMAL_CLEARING |
| 0x11 | USER_BUSY |
| 0x12 | NO_USER_RESPONDING |
| 0x13 | NO_USER_ANSWER |
| 0x15 | CALL_REJECTED |
| 0x16 | NUMBER_CHANGED |
| 0x1a | NON_SELECTED_CLEARING |
| 0x1b | DEST_OUT_OF_ORDER |
| 0x1c | INVALID_NUMBER_FORMAT |
| 0x1d | FACILITY_REJECTED |
| 0x1e | RESP_TO_STAT_ENQ |
| 0x1f | UNSPECIFIED_CAUSE |

*Table 6-7 Cause Values and Definitions (continued)*

| Hexadecimal Value | Cause Definitions |
|---|---|
| 0x22 | NO_CIRCUIT_AVAILABLE |
| 0x26 | NETWORK_OUT_OF_ORDER |
| 0x29 | TEMPORARY_FAILURE |
| 0x2a | NETWORK_CONGESTION |
| 0x2b | ACCESS_INFO_DISCARDED |
| 0x2c | REQ_CHANNEL_NOT_AVAIL |
| 0x2d | PRE_EMPTED |
| 0x2f | RESOURCES_UNAVAILABLE |
| 0x32 | FACILITY_NOT_SUBSCRIBED |
| 0x33 | BEARER_CAP_INCOMPAT |
| 0x34 | OUTGOING_CALL_BARRED |
| 0x36 | INCOMING_CALL_BARRED |
| 0x39 | BEARER_CAP_NOT_AUTH |
| 0x3a | BEAR_CAP_NOT_AVAIL |
| 0x3b | CALL_RESTRICTION |
| 0x3c | REJECTED_TERMINAL |
| 0x3e | SERVICE_NOT_ALLOWED |
| 0x3f | SERVICE_NOT_AVAIL |
| 0x41 | CAP_NOT_IMPLEMENTED |
| 0x42 | CHAN_NOT_IMPLEMENTED |
| 0x45 | FACILITY_NOT_IMPLEMENT |
| 0x46 | BEARER_CAP_RESTRICTED |
| 0x4f | SERV_OPT_NOT_IMPLEMENT |
| 0x51 | INVALID_CALL_REF |
| 0x52 | CHAN_DOES_NOT_EXIST |
| 0x53 | SUSPENDED_CALL_EXISTS |

*Table 6-7 Cause Values and Definitions (continued)*

| Hexadecimal Value | Cause Definitions |
|---|---|
| 0x54 | NO_CALL_SUSPENDED |
| 0x55 | CALL_ID_IN_USE |
| 0x56 | CALL_ID_CLEARED |
| 0x58 | INCOMPATIBLE_DEST |
| 0x5a | SEGMENTATION_ERROR |
| 0x5b | INVALID_TRANSIT_NETWORK |
| 0x5c | CS_PARAMETER_NOT_VALID |
| 0x5f | INVALID_MSG_UNSPEC |
| 0x60 | MANDATORY_IE_MISSING |
| 0x61 | NONEXISTENT_MSG |
| 0x62 | WRONG_MESSAGE |
| 0x63 | BAD_INFO_ELEM |
| 0x64 | INVALID_ELEM_CONTENTS |
| 0x65 | WRONG_MSG_FOR_STATE |
| 0x66 | TIMER_EXPIRY |
| 0x67 | MANDATORY_IE_LEN_ERR |
| 0x6f | PROTOCOL_ERROR |
| 0x7f | INTERWORKING_UNSPEC |

# Call Scenarios for the POTS Dial Feature

This section describes three call scenarios and shows examples of the Cisco IOS command output for each scenario. The output examples for the **debug** and **disconnect** commands show the sequence of events that occur during a POTS dial call.

## Call Scenario 1

In this call scenario, port 1 is on-hook, the application dial is set to call 4085552221, and the far end successfully connects. The following example shows the Cisco IOS command:

```
router# test pots 1 dial 4085552221#
router#
```

The following screen output shows an event indicating that port 1 is being used by the dial application:

```
01:0, port = 1
```

The following screen output shows events indicating that the CSM is receiving the application digits of the number to dial:

```
01:58:27: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:58:27: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:58:27: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:58:27: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:58:27: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:58:27: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:58:27: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:58:27: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:58:27: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:58:27: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
```

The following screen output shows that the telephone connected to port 1 is off hook:

```
01:58:39: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_OFFHOOK, call id = 0x0, port = 1
```

The following screen output shows a call-proceeding event pair indicating that the router ISDN software has sent the dialed digits to the ISDN switch:

```
01:58:40: EVENT_FROM_ISDN:dchan_idb=0x280AF38, call_id=0x8004, ces=0x1 bchan=0x0,
event=0x3, cause=0x0
01:58:40: CSM_PROC_ENBLOC_DIALING: CSM_EVENT_ISDN_PROC, call id = 0x8004, port = 1
```

The following screen output shows the call-progressing event pair indicating that the telephone at the far end is ringing:

```
01:58:40: EVENT_FROM_ISDN:dchan_idb=0x280AF38, call_id=0x8004, ces=0x1 bchan=0xFFFFFFFF,
event=0x5, cause=0x0
01:58:40: CSM_PROC_ENBLOC_DIALING: CSM_EVENT_ISDN_CALL_PROGRESSING, call id = 0x8004, port
= 1
```

The following screen output shows a call-connecting event pair indicating that the telephone at the far end has answered:

```
01:58:48: EVENT_FROM_ISDN:dchan_idb=0x280AF38, call_id=0x8004, ces=0x1 bchan=0xFFFFFFFF,
event=0x4, cause=0x0
01:58:48: CSM_PROC_CONNECTING: CSM_EVENT_ISDN_CONNECTED, call id = 0x8004, port = 1
```

The following screen output shows a call-progressing event pair indicating that the telephone at the far end has hung up, and the calling telephone is receiving an in-band tone from the ISDN switch:

```
01:58:55: EVENT_FROM_ISDN:dchan_idb=0x280AF38, call_id=0x8004, ces=0x1 01:58:55:
CSM_PROC_CONNECTED: CSM_EVENT_ISDN_CALL_PROGRESSING,
call id = 0x8004, port = 1
```

The following screen output shows that the telephone connected to port 1 has hung up:

```
01:58:57: CSM_PROC_CONNECTED: CSM_EVENT_VDEV_ONHOOK, call id = 0x8004, port = 1
```

The following screen output shows an event pair indicating that the call has been terminated:

```
01:58:57: EVENT_FROM_ISDN:dchan_idb=0x280AF38, call_id=0x8004, ces=0x1 bchan=0xFFFFFFFF,
event=0x0, cause=0x0
01:58:57: CSM_PROC_NEAR_END_DISCONNECT: CSM_EVENT_ISDN_DISCONNECTED, call id = 0x8004,
port = 1
813_local#
```

## Call Scenario 2

In this scenario, port 1 is on-hook, the application dial is set to call 4085552221, and the destination number is busy. The following example shows the Cisco IOS command:

```
router# test pots 1 dial 4085552221#
router#
```

The following screen output shows that your dial application is using port 1:

```
01:59:42: CSM_PROC_IDLE: CSM_EVENT_VDEV_APPLICATION_CALL, call id = 0x0, port = 1
```

The following screen output shows the events indicating that the CSM is receiving the application digits of the number to call:

```
01:59:42: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id =
0x0, port = 1
```

```
01:59:42: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:59:42: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:59:42: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:59:42: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:59:42: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:59:42: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:59:42: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:59:42: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:59:42: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
```

The following screen output shows an event indicating that the telephone connected to port 1 is off-hook:

```
01:59:52: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_OFFHOOK, call id = 0x0, port = 1
```

The following screen output shows a call-proceeding event pair indicating that the telephone at the far end is busy:

```
01:59:52: EVENT_FROM_ISDN:dchan_idb=0x280AF38, call_id=0x8005, ces=0x1 bchan=0x0,
event=0x3, cause=0x11
01:59:52: CSM_PROC_ENBLOC_DIALING: CSM_EVENT_ISDN_PROC, call id = 0x8005, port = 1
```

The following screen output shows a call-progressing event pair indicating that the calling telephone is receiving an in-band busy tone from the ISDN switch:

```
01:59:58: EVENT_FROM_ISDN:dchan_idb=0x280AF38, call_id=0x8005, ces=0x1 bchan=0xFFFFFFFF,
event=0x5, cause=0x0
01:59:58: CSM_PROC_ENBLOC_DIALING: CSM_EVENT_ISDN_CALL_PROGRESSING, call id = 0x8005, port
= 1
```

The following screen output shows an event indicating that the calling telephone has hung up:

```
02:00:05: CSM_PROC_ENBLOC_DIALING: CSM_EVENT_VDEV_ONHOOK, call id = 0x8005, port = 1
```

The following screen output shows an event pair indicating that the call has terminated:

```
02:00:05: EVENT_FROM_ISDN:dchan_idb=0x280AF38, call_id=0x8005, ces=0x1 bchan=0xFFFFFFFF,
event=0x0, cause=0x0
02:00:05: CSM_PROC_NEAR_END_DISCONNECT: CSM_EVENT_ISDN_DISCONNECTED, call id = 0x8005,
port = 1
```

## Call Scenario 3

In this call scenario, port 1 is on-hook, the application dial is set to call 4086661112, the far end successfully connects, and the command **test pots disconnect** terminates the call.

```
router# debug pots csm
router# test pots 1 dial 4086661112
router#
```

The following screen output follows the same sequence of events as shown in Call Scenario 1:

```
1d03h: CSM_PROC_IDLE: CSM_EVENT_VDEV_APPLICATION_CALL, call id = 0x0, port = 1
1d03h: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
1d03h: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
1d03h: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
1d03h: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
1d03h: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
1d03h: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
1d03h: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
1d03h: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
1d03h: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
1d03h: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1

1d03h: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_OFFHOOK, call id = 0x0, port = 1

1d03h: EVENT_FROM_ISDN:dchan_idb=0x2821F38, call_id=0x8039, ces=0x1
   bchan=0x0, event=0x3, cause=0x0
1d03h: CSM_PROC_ENBLOC_DIALING: CSM_EVENT_ISDN_PROC, call id = 0x8039, port = 1

1d03h: EVENT_FROM_ISDN:dchan_idb=0x2821F38, call_id=0x8039, ces=0x1
   bchan=0xFFFFFFFF, event=0x5, cause=0x0

1d03h: CSM_PROC_ENBLOC_DIALING: CSM_EVENT_ISDN_CALL_PROGRESSING, call id = 0x8039,
    port = 1

router# test pots 1 disconnect
```

The **test pots disconnect** command disconnects the call before you have to put the telephone back on hook.

```
1d03h: CSM_PROC_CONNECTING: CSM_EVENT_VDEV_APPLICATION_HANGUP_CALL, call id = 0x8039,
     port = 1
1d03h: EVENT_FROM_ISDN:dchan_idb=0x2821F38, call_id=0x8039, ces=0x1
   bchan=0xFFFFFFFF, event=0x0, cause=0x0
```

```
1d03h: CSM_PROC_DISCONNECTING: CSM_EVENT_ISDN_DISCONNECTED, call id = 0x8039,
    port = 1
1d03h: CSM_PROC_DISCONNECTING: CSM_EVENT_TIMEOUT, call id = 0x8039, port = 1
```

# Cisco 813 Router Enhanced Voice Features (Japan Only)

The Cisco 813 router supports the enhanced voice features in addition to the standard voice features of the Ciso 800 series routers. The enhanced voice features were developed to work with the INS-NET-64 switch used by Nippon Telephone and Telegraph (NTT).

Support for these features is limited to Japanese telephones, with the exception of the call blocking on caller ID feature. For more information about each feature, see the following topics:

- General Requirements and Restrictions
- Caller ID Display
- Call Blocking on Caller ID
- Local Call Waiting
- E Ya Yo
- Voice Warp
- Voice Select Warp
- Nariwake
- Trouble-Call Blocking
- I Number

# General Requirements and Restrictions

The following is a list of requirements for activating the enhanced voice features on the Cisco 813 router:

- Subscription to the NTT INS-NET-64 switch type.
- Configuration of the router telephone ports to the Japanese standards by using the Cisco IOS command **pots country** *jp*.

# Caller ID Display

This feature displays the caller ID information provided by the INS-NET-64 switch on analog telephones connected to the PHONE 1 or 2 port of the Cisco 813 router.

## Requirements for Activating Caller ID Display

The following is a list of requirements for activating this feature:

- Subscription to the caller ID service
- Subscription to the INS-NET-64 switch
- Configuration of the router using the Cisco IOS command **pots country** *jp*

**Note** The caller ID display feature works only on Japanese language display telephones.

## Configuring Caller ID Display

By default, this feature is disabled. To configure this feature, use the Cisco IOS **caller-id enable** command in the dial-peer configuration command mode.

```
caller-id enable
no caller-id enable
```

# Call Blocking on Caller ID

This feature can reject an incoming voice call based on the caller ID information presented to the Cisco 813 router from the INS-NET-64 switch. This feature can block calls for up to ten caller IDs for each local directory number (LDN).

## Requirements for Activating Call Blocking on Caller ID

The following requirements must be met before activating this feature:

- Subscription to the caller ID service on the INS-NET-64 switch. If this feature is enabled on the router without the caller ID subscription, the router will neither verify telephone numbers from callers nor block their calls.
- Configuration of the router using the Cisco IOS command **pots country** *jp*.

## Configuring Call Blocking on Caller ID

By default, this feature is disabled. To configure this feature, use the Cisco IOS **block-caller** command in the dial-peer configuration command mode.

```
block-caller number
no block-caller
```

where *number* is the telephone number to block. You can use a period (.) as a wildcard to substitute for one or more numbers to block. For example, to block all numbers ending in the number 5, you can enter the following:

```
block-caller .5
```

You can enter up to ten caller ID numbers for each LDN. However, you cannot exceed the maximum of ten numbers. You must remove one or more numbers before you can add any new numbers to block.

If no caller ID numbers are specified for a particular LDN, all voice calls to that LDN are accepted.

### Example of Caller ID Blocking Configuration

The following example configures the router to block calls from the caller whose caller ID number is 4085551234:

```
router(config)# pots country jp
router(config)# dial-peer voice 1 pots
router(config-dial-peer)# block-caller 4085551234
```

### Example of Caller ID Blocking Output

To display caller IDs entered for call blocking, use the **show run** command. The following is an example of caller ID configuration output:

```
!
dial-peer voice 1 pots
no forward-to-unused-port
call waiting
ring 0
registered-caller ring 1
port 1
block-caller 4085551234
block-caller 4085552345
```

## Local Call Waiting

This feature notifies you of an incoming call while you are connected to an external telephone call (by issuing a call waiting tone). You can choose to place the first call on hold by pressing flash, connect to the second call, then return to the first call after finishing with the second.

Local call waiting on the Cisco 813 router differs from standard ISDN call waiting in that this enhanced voice feature does not require a subscription to call waiting from the service provider. This feature uses both B channels of the ISDN line, enabling local call waiting support on the router rather than from the service provider.

This feature is not supported if any of the interactive voice response (IVR) features (such as voice warp, voice select warp, and Nariwake) are in use.

## Requirements for Activating Local Call Waiting

The following requirements must be met before activating this feature:

- Subscription to any telephone service provider switch
- Configuration of the router using the Cisco IOS command **pots country** *jp*

## Configuring Local Call Waiting

To configure this feature, use the Cisco IOS **pots call-waiting** command:

```
pots call-waiting [local|remote]
```

The call waiting defaults to **remote** if this feature is not configured. In that case, the call holding pattern follows the settings of the service provider rather than those of the router.

To display the call waiting setting, use the **show run** or **show pots status** command.

**Note** The ISDN call waiting service will be used if it is available on the ISDN line connected to the router even if local call waiting is configured on the router. If ISDN call waiting is used, the local call waiting configuration on the router is ignored.

### Example of Local Call Waiting Configuration

The following example configures the call waiting style to follow the local call holding pattern that is set on the router:

```
router(config)# pots country jp
router(config)# pots call-waiting local
```

# E Ya Yo

This feature conceals the caller ID of the outgoing call from the receiving device.

## Requirements for Activating E Ya Yo

The following requirements must be met before activating this feature:

- Subscription to the E Ya Yo service
- Subscription to the INS-NET-64 switch
- Configuration of the router using the Cisco IOS command **pots country** *jp*

## Configuring E Ya Yo

According to the NTT specification, dialing the prefix **184** followed by the destination device number will render your caller ID invisible to the receiving party.

# Voice Warp

The voice warp feature on the INS-NET-64 switch forwards all incoming calls for a terminal device to another device. Voice warp registration, activation, and deactivation requests are sent to the switch for each LDN. The Cisco 813 router supports the registration, activation, and deactivation requests for any device attached to the PHONE 1 or 2 port. The forwarding function itself is performed by the INS-NET-64 switch.

During the registration phase of the device, you can:

- Create a list of forwarding destination numbers and to select one as the active destination.
- Specify whether an announcement will be made to the caller or forwarding device, or both, at the time the call is forwarded.
- Set the no-answer timer parameter from 5 to 60 seconds at 5-second intervals. This setting affects the redirection of calls once the voice warp feature is activated.

During the activation phase of this feature, you determine whether calls are redirected all the time or only if the receiving device is busy or does not answer within the no-answer time period specified during registration.

This feature can be deactivated after its registration and activation phases.

**Note** The Cisco 813 router supports this feature for one LDN only. If more than one LDN is configured, only the primary LDN can be used with this feature.

## Requirements for Activating Voice Warp

The following requirements must be met before activating this feature:

- Subscription to the voice warp and caller ID services
- Subscription to the INS-NET-64 switch
- Configuration of the router using the Cisco IOS command **pots country** *jp*

**Note** Activating the voice warp feature disables the support for the call waiting feature for both local and network calls.

## Configuring Voice Warp

This feature is configured using the interface on the telephone as specified in the NTT user manual.

To hear the voice warp registration details of a device, use the keypad dialing sequence specified in the NTT user manual. Information is transmitted only by voice.

## Voice Select Warp

This feature is an enhanced version of the voice warp feature. You can create a list of incoming caller IDs that is used in call redirection, either by redirecting incoming calls only from matching caller IDs, or by redirecting all calls except those from matching caller IDs.

Note The Cisco 813 router supports this feature for one LDN only. If more than one LDN is configured, only the primary LDN can be used with this feature.

## Requirements for Activating Voice Select Warp

The following requirements must be met before activating this feature:

- Subscription to the voice select warp and caller ID services
- Subscription to the INS-NET-64 switch
- Configuration of the router using the Cisco IOS command **pots country** *jp*

Note Activating the voice select warp feature disables the support for the call waiting feature for both local and network calls.

## Configuring Voice Select Warp

This feature is configured using the interface on the telephone as specified in the NTT user manual.

To get voice warp registration details of a device, use the keypad dialing sequence specified in the NTT user manual. Information is transmitted only by voice.

# Nariwake

Nariwake checks for caller IDs that you register for each LDN and presents a distinctive ring to the telephone port receiving the incoming call if a match is detected. The Cisco 813 router provides three different ring cadences that you can set for calls from registered and unregistered callers. The number of caller IDs you can register for each LDN at one time is defined by the INS-NET-64 switch and not by the router.

You can register this feature with the list of caller IDs for each LDN, cancel the registration for the LDN, or get registration information from the INS-NET-64 switch.

**Note** The Cisco 813 router supports this feature for one LDN only. If more than one LDN is configured, only the primary LDN can be used with this feature.

## Requirements for Activating Nariwake

The following requirements must be met before activating this feature:

- Subscription to the Nariwake feature
- Subscription to the INS-NET-64 switch
- Configuration of the router using the Cisco IOS command **pots country** *jp*

**Note** Activating the Nariwake feature disables support for the call waiting feature for both local and network calls.

## Configuring Nariwake

To configure the ring cadence for this feature, use the **registered-caller ring** command in the dial-peer configuration mode:

```
registered-caller ring cadence
```

where *cadence* is a value of 0, 1, or 2. The default ring cadence for registered callers is 1 and for unregistered callers is 0.

The on/off periods of ring 0 (normal ringing signals) and ring 1 (ringing signals for the Nariwake service) are defined in the NTT user manual.

**Note** If your ISDN line is provisioned for the I Number or dial-in services, you must also configure a dial-peer using the Cisco IOS command **destination-pattern not-provided.** Either port 1 or 2 can be configured under this dial-peer. The router will then forward the incoming call to the voice port 1 using the default cadence 0. See the "Example of Nariwake Configuration" section for details.

If more than one dial-peer is configured with **destination-pattern not-provided**, the router uses only the first dial-peer for the incoming calls.

To hear the caller ID registration details, use the keypad dialing sequence specified in the NTT user manual. Information is transmitted only by voice.

### Example of Nariwake Configuration

The following example sets the ring cadence for registered callers to 2.

```
router(config)# pots country jp
router(config)# dial-peer voice 1 pots
router(config-dial-peer)# registered-caller ring 2
```

Add the **destination-pattern not-provided** command if you also subscribe to the I Number and dial-in services.

```
router(config-dial-peer)# destination-pattern not-provided
```

### Example of Nariwake Configuration Output

To display the Nariwake ring cadence setting, use the **show run** command. The following is an example of screen output for Nariwake configuration:

```
dial-peer voice 1 pots
no forward-to-unused-port
call waiting
ring 0
registered-caller ring 2
port 1
destination-pattern not-provided
block-caller 4085552222
block-caller 4085553333
```

## Trouble-Call Blocking

The trouble-call blocking feature causes all future incoming calls from a particular telephone number to be rejected by the network if the recipient activates this feature after the initial call. As the recipient of the call, you are not required to specify the telephone number of the caller and will not be notified of subsequent connection attempts from that telephone number. When this feature is activated, the caller will hear a standard telephone announcement and a disconnect message. For information about the announcement or message, see your NTT user manual.

The number of callers that you can block is defined by the service provider at the time the service is provisioned. If you request an additional telephone number to block after having reached the limit, the oldest number is discarded (unblocked) before the latest telephone number is registered for blocking.

## Requirements for Activating Trouble-Call Blocking

The following requirements must be met before activating this feature:

- Subscription to the trouble-call blocking feature
- Subscription to the INS-NET-64 switch
- Configuration of the router using the Cisco IOS command **pots country** *jp*

## Configuring Trouble-Call Blocking

You can activate, cancel, or request confirmation of the results of your trouble-call blocking by using the keypad dialing sequence specified in the NTT user manual.

**Note** To activate this feature, you must dial the keypad sequence within 60 seconds after you hang up from the call. You will be notified over the telephone whether or not the activation is successful.

You can disable this feature for only the last registered number or for all numbers registered for blocking. You will be notified over the telephone whether or not the cancellation is successful.

You can request to hear the results of the trouble-call blocking. You will hear the number of attempted calls that were blocked for the past two months.

# I Number

This feature supports the use of multiple terminal devices with one subscriber line. The telephone numbers of the subscriber line and router ports are assigned by the service provider. Calls coming into any of the assigned numbers will route through the same subscriber line to the terminal device attached to the target port.

## Requirements for Activating I Number

The following requirements must be met before activating this feature:

- Subscription to the I number feature
- Subscription to the INS-NET-64 switch
- Configuration of the router using the Cisco IOS command **pots country** *jp*

## Configuring I Number

To configure this feature, perform the following steps:

**Step 1** Use the **isdn i-number** command in the BRI interface configuration mode to configure the I number:

```
isdn i-number number ldn
```

where *number* is a value from 1 to 3 (based on NTT specifications) and *ldn* is your local directory number configured under the dial-peer. The *number* variable maps the I number to one of the LDNs.

**Step 2** Use the **destination-pattern** command to set the dial-peer destination pattern to the corresponding LDN:

```
destination-pattern ldn
```

### Example of I Number Configuration

The following example shows screen output for two LDNs configured under interface BRI0:

```
router(config)# interface bri0
router(config-if)# isdn i-number 1 5551234
router(config-if)# isdn i-number 2 5556789
router(config-if)# exit
router(config)# dial-peer voice 1 pots
router(config-dial-peer)# destination-pattern 5551234
router(config-dial-peer)# exit
router(config)# dial-peer voice 2 pots
router(config-dial-peer)# destination-pattern 5556789
```

# Silent Fax Calls

The silent fax calls feature enables you to configure your router port to send a silent fax tone instead of a ring alert, which is recognized by fax machines with silent fax recognition capability (Smart Fax type 2). With the silent fax feature, the fax machine does not ring but the fax call get connected. If a phone is connected instead of a fax machine, the phone will not ring.

## Configuring Silent Fax Calls

To configure your telephone port as a silent fax type 2, use the Cisco IOS **silent-fax** command in dial-peer configuration mode:

```
silent-fax
no silent-fax
```

By default, this feature is disabled.

## Example of Silent Fax Calls Configuration

The following is an example of a silent fax call configuration:

```
router# configure terminal
router(config)# dial-peer voice 1 pots
router(config-dial-peer)# silent-fax
```

## Example of Silent Fax Calls Configuration Output

The following is an example of the silent fax configuration output:

```
dial-peer voice 1 pots
  caller-id
  no forward-to-unused-port
  call-waiting
  ring 0
  no silent-fax
  registered-caller ring 1
  port 1
  volume 3
  destination-pattern 7773000
!
dial-peer voice 2 pots
```

```
  caller-id
  no forward-to-unused-port
  call-waiting
  ring 0
  no silent-fax
  registered-caller ring 1
  port 2
  volume 3
  destination-pattern 7773100
!
```

# Supplementary Telephone Services for the Net3 Switch

The Cisco 800 series routers now support the following plain old telephone service (POTS) features for the European Telecommunications Standards Institute (ETSI) Net3 switch type:

- Caller ID presentation and restriction are available for Denmark and Finland. For more information, see the "Configuring Caller ID for the Net3 Switch" section on page 6-47.
- Calling line identification restriction (CLIR) temporarily prevents your calling ID from being presented to the destination number for an outgoing call. You must configure CLIR before each call that you wish to restrict.
- Call forwarding is enabled by using Cisco IOS and dual tone multifrequency (DTMF) commands. For more information, see the "Call Forwarding for the Net3 Switch" section on page 6-48.
- Call transfer enables you to connect two call destinations. The request for this service must originate from an active, outgoing call.

## Requirements for Supplementary Telephone Services Support

You must subscribe to the following Net3 switch services for these supplementary telephone services to work:

- Calling line identification presentation (CLIP)
- CLIR in temporary mode

- Call holding
- Call transfer
- Call forwarding
- Call waiting

## Configuring Caller ID for the Net3 Switch

To enable caller ID on the Net3 switch, configure the country type by using the Cisco IOS **pots country** command in global configuration mode:

```
pots country {dk|fi}
```

**Note** Caller ID for the Net3 switch is always enabled, provided that the POTS country type is correctly defined. Caller ID cannot be disabled using the Cisco IOS command-line interface (CLI).

To verify whether caller ID is enabled, use the **show pots status** command. The following is an example of the output from that command:

```
router# show pots status

POTS Global Configuration:

   Country:Denmark

   Dialing Method:Overlap, Tone Source:Local, CallerId Support:YES
        ----------------------
   Out Going Hunt:Disabled
```

# Call Forwarding for the Net3 Switch

The following types of call forwarding services (for voice calls only) are supported on the Net3 switch:

- Call forward unconditional (CFU) redirects your calls without restrictions and takes precedence over other call forwarding types.
- Call forward busy (CFB) redirects your call to another number if your number is busy.
- Call forward no reply (CFNR) forwards your call to another number if your number does not answer within a specified period of time.

You can select one or more call forwarding services at a time. However, CFU has the highest precedence, CFB the next highest, and CFNR the lowest. The default setting is that no forwarding type is selected.

**Note** If you had configured call forwarding for a POTS port and the router finds that a dial peer is also configured for that port, call forwarding works only for the number defined in the **destination-pattern** dial-peer command and ignores all other numbers for that telephone. If the router does not find a dial peer, or if the destination pattern is not defined, call forwarding works for all numbers allocated to the ISDN line.

To enable and configure this feature, follow these steps:

**Step 1** Enable and select the call forwarding method. See the "Configuring the Call Forwarding Method" section on page 6-49.

**Step 2** Configure your call forwarding service, depending on which method you previously selected:

- Functional method—Enter DTMF commands on the telephone keypad. For more information, see the "Configuring the Call Forwarding Service" section on page 6-49.
- Keypad method—Follow the instructions in your Net3 switch documentation.

## Configuring the Call Forwarding Method

You can select the method by which the call forwarding feature is controlled:

- Functional method gives control to the router. If you select this method, use the DTMF commands documented in the "Configuring the Call Forwarding Service" section on page 6-49.
- Keypad method gives control to the Net3 switch.

To enable the call forwarding method, use the Cisco IOS **pots forwarding-method** command in global configuration mode:

```
pots forwarding-method {functional | keypad}
no pots forwarding-method
```

**Note** Use the **pots forwarding-method** command to configure only Net3 switch types. This command does not work for other switch types. This feature is disabled in the default setting.

The following example configures the call forwarding feature to give control to the router:

```
router# configure terminal
router(config)# pots forwarding-method functional
```

## Configuring the Call Forwarding Service

Table 6-8 shows the DTMF keypad command sequence that you enter to configure the call forwarding service.

*Table 6-8 Configuring the Call Forwarding Service*

| Task | DTMF Keypad Command |
|---|---|
| Activate CFU | `**21*`*`number`*`#`<br>where *number* is the telephone number to which your calls are forwarded |
| Deactivate CFU | `#21#` |

*Table 6-8 Configuring the Call Forwarding Service (continued)*

| Task | DTMF Keypad Command |
|---|---|
| Activate CFNR | ****61****number***#**<br>where *number* is the telephone number to which your calls are forwarded |
| Deactivate CFNR | **#61#** |
| Activate CFB | ****67****number***#**<br>where *number* is the telephone number to which your calls are forwarded |
| Deactivate CFB | **#67#** |

You should hear a dial tone after you enter the DTMF commands if the call forwarding service is successfully configured. If you hear a busy signal, the command is invalid or the switch does not support that service.

## Displaying POTS Status

Use the **show pots status** command to display details of the call forwarding type. This status is not stored when you reboot. The following is an example of the screen output:

```
router# show pots status

POTS Global Configuration:
Country:Denmark
Dialing Method:Overlap, Tone Source:Local, CallerId Support:YES
Out Going Hunt:Disabled
Forwarding Method:functional method
-------------------------------------

Call Forwarding status:

The Forwarding Method Enabled is CFU

The forwarded to Address is     :33236877
The served user Number(s) are   :33795742

The Forwarding Method Enabled is CFB
The forwarded to Address is     :33236877
The served user Number(s) are   :
   ALL -> Will work for all numbers allocated to the terminal.
```

## Configuring CLIR

Configure CLIR by following these steps:

**Step 1** Ensure that CLIR in temporary mode is enabled in the Net3 switch.

**Step 2** Remove the handset and enter ****31#** on the keypad.

**Step 3** Listen for the dial tone, and make your call.

**Step 4** Repeat Steps 2 and 3 for each outgoing call for which you wish to restrict your calling identification.

## Debug POTS Commands

Use the following commands to debug problems with caller ID configuration:

- **debug pots driver**
- **debug pots csm**

Use the following commands for problems configuring other supplementary telephone features:

- **debug pots csm**
- **debug isdn event**
- **debug isdn q931**

For more information about using debug commands, refer to the Cisco IOS documentation.

# Cisco 804 and 813 Routers Enhanced Voice Features

The Cisco 804 and 813 routers support the following enhanced voice features. For information on each feature, see the following topic:

- Prefix Dialing
- Calling Between Telephone Ports
- Redial
- Call Transfer
- Volume Adjustments
- Distinctive Ringing Based on Caller ID
- Subaddresses for POTS Ports
- Caller ID on the Cisco 813 Router

## Prefix Dialing

Cisco 803 and Cisco 804 routers support prefix dialing. You can add a telephone prefix and create a prefix filter to the dialed number for analog telephone calls. When a telephone number is dialed through the telephone port, the router checks for prefix filters. If the router finds a match, no prefix is added to the dialed number. If no filter match is found, the router adds the user-defined prefix to the called number.

### Configuring a Prefix Number

To set a prefix to be added to a telephone number called, use the Cisco IOS **pots prefix number** command in global configuration mode:

```
pots prefix number number
no pots prefix number
```

where *number* is a prefix number from 1 to 5 digits in length. Only one prefix can be configured at a time, and configuring a new number will overwrite the existing one.

The following example sets the prefix number to 12345*:*

```
router# configure terminal
router(config)# pots prefix number 12345
```

## Configuring a Prefix Filter

You can configure a prefix filter that is compared to the digits that you dial. If a match occurs, the prefix number is not added to the called number. To create a prefix filter, use the **pots prefix filter** command in global configuration mode:

```
pots prefix filter number
no pots prefix filter number
```

where *number* is a prefix filter from 1 to 8 digits in length. You can define up to ten filters for your router. If you have reached the maximum number of filters defined, no new filter configurations are accepted until you remove at least one existing filter number using the **no pots prefix filter** *number* command.

The following are examples of how to set prefix filters:

```
router# configure terminal
router(config)# pots prefix filter 192
router(config)# pots prefix filter 1
router(config)# pots prefix filter 9
router(config)# pots prefix filter 0800
router(config)# pots prefix filter 08456
```

# Calling Between Telephone Ports

The calling between telephone ports voice feature enables a connection between the two telephone ports of your router. This voice call is handled by the router and does not affect any data calls handled on the B channels. However, the following restrictions apply:

- During a call between ports, an incoming voice call cannot supersede the data calls. The router sends a disconnect message to the network for incoming voice calls.
- If voice priority is set on the router and two data calls are in progress, an attempted call between ports takes precedence over one of the data calls. This applies to the overlap mode of dialing.

- The call waiting tone is not activated for the local telephone ports even if call waiting is enabled locally or at the switch. An external calling party hears a busy tone if the telephone ports are engaged.

## Activating the Calling Between Telephone Ports Feature

To make a call between telephone ports, press ****0#** on your telephone handset.

## Calling Between Telephone Ports Scenarios

Table 6-9 shows scenarios for calling between telephone ports.

*Table 6-9 Scenarios for Calling Between Telephone Ports*

| POTS 1 | POTS 2 | B1 Channel | B2 Channel | Command | Result |
|---|---|---|---|---|---|
| IDLE | IDLE | Free | Free | Press ****0#** from POTS 1 or POTS 2 | Intercom call is established. |
| IDLE | IDLE | Data call in progress | Free | Press ****0#** from POTS 1 or POTS 2 | Intercom call is established. |
| IDLE | IDLE | Data call in progress | Data call in progress | Press ****0#** from POTS 1 or POTS 2 | Intercom call is established. But in overlap mode, one data call is bumped |
| IDLE | IDLE | Data call in progress | Data call in progress | Press ****0#** from POTS 1 or POTS 2 | Intercom call is established successfully in enblock mode. User gets busy tone in overlap mode. |

*Table 6-9 Scenarios for Calling Between Telephone Ports (continued)*

| POTS 1 | POTS 2 | B1 Channel | B2 Channel | Command | Result |
|---|---|---|---|---|---|
| IDLE | IDLE | Data call in progress | Data call in progress | Press ****0#** from POTS 1 or POTS 2 | Telephone port call is established successfully in enblock mode. In overlap mode, if both the calls aredestined for same location, then one data call is bumped to establish the intercom mode successfully. Otherwise, the user at POTS 1 or 2 hears a busy tone. |
| Intercom | Intercom | Free | Free | Press **flash** and any key at POTS 1 | During the intercom call flashhook/keys is not detected. |
| Intercom | Intercom | Free/data call | Free/data call | An external voice call comes to POTS 1 | No call waiting tone is generated and the external user hears a busy tone. Data calls are not bumped. |
| IDLE | External voice call | Voice call | Free | Press ****0#** from POTS 1 | Intercom fails and user hears a busy tone. |
| IDLE | External voice call | Voice call | Data call in progress | Press ****0#** from POTS 1 | Intercom fails and the user hears a busy tone. In overlap mode, the data call is bumped. |
| IDLE | External voice call | Voice call | Data call in progress | Press ****0#** from POTS 1 | Intercom fails and the user hears a busy tone. |

# Redial

This feature enables you to redial the last number called on either telephone port 1 or 2. The following conditions apply:

- This feature recalls only the last digits dialed, to a maximum of 65.
- The router does not store feature access codes starting with an asterisk (*), interactive voice response (IVR) digits, or the pound (#) key.

## Activating the Redial Feature

To redial the last number called, press ****4#** on your telephone handset.

## Redial Feature Scenarios

Table 6-10 shows scenarios for the redial feature.

*Table 6-10 Scenarios for Redial Feature*

| Event/Condition | Command | Result |
|---|---|---|
| User dialed external number from POTS 1 or POTS 2. | Press ****4#** from POTS 1 or POTS 2. | The last number dialed from POTS port 1 or POTS port 2 is called again. |
| User invoked a DTMF function for POTS 1 or POTS 2 on a per call basis and then pressed the actual number for a dialing connection. | Press ****4#** from POTS 1 or POTS 2. | Only the actual called number gets redialed and not the input for the DTMF function. |
| The previous call was between POTS ports on the same router. Now the user dials the required digits for IVR. | Press ****4#** from POTS 1 or POTS 2 | No number is stored for redial. No number is dialed, and the user only hears a dial tone. |

# Call Transfer

The call transfer feature enables you to transfer an external call from one telephone port to the other. Call transfer does not require any subscription from the switch.

## Activating the Call Transfer Feature

To transfer an incoming voice call from one port to another, press the flash hook switch, then ****0#** on the telephone handset.

## Call Transfer Feature Scenarios

Table 6-11 shows scenarios for call transfer.

*Table 6-11 Scenarios for Call Transfer*

| Event/Condition | Called Port | Command | Result |
|---|---|---|---|
| External caller dialed POTS 1 or POTS 2 port and the user decides to transfer the call to the other port. | IDLE | Press flash hook switch and ****0#** from POTS 1 or POTS 2. | The connection is established between the external caller and POTS 1 or POTS 2 when the handset connected to the other POTS port goes to onhook. |
| External caller dialed POTS 1 or POTS 2 port. POTS 1 or POTS 2 decides to transfer the call to the other port, but that port is busy with a call. | BUSY | Press FLASH ****0#** from POTS 1 or POTS 2. | No connection is established between POTS 1 and POTS 2. The connection between the external call and called POTS port is still valid, so the user can resume conversation with the external called by pressing **FLASH**. |

*Table 6-11 Scenarios for Call Transfer (continued)*

| Event/Condition | Called Port | Command | Result |
|---|---|---|---|
| External caller dialed POTS 1 or POTS 2. The user decides to transfer the call to the other port and keep the phone on hook without checking the availability of the port. | IDLE | Press FLASH ****0#** from POTS 1 or POTS 2 | This is an example of an unsupervised call and is not supported. No connection will be made between the external caller and the port to which they are being transferred. |

# Volume Adjustments

The volume adjustment features enables you to adjust the receiver volume of the POTS ports.

To configure the telephone receiver volume on each port, use the Cisco IOS **volume** command in the dial-peer configuration mode:

```
volume number
```

where *number* is a numeric value from 1 to 5 representing the volume setting

ranging from -12 to 0 decibels (dB). The default setting is 3.

Table 6-12 lists the values and definitions of the *number* variable.

*Table 6-12 Volume Adjustment Number Variable Definitions*

| Number | Volume Setting in dB |
|---|---|
| 1 | -12 |
| 2 | -9 |
| 3 | -6 |
| 4 | -3 |
| 5 | 0 |

## Volume Adjustment Configuration Example

The following example configures the volume of the receiver on the router telephone ports 1 and 2:

```
router# configure terminal
router(config)# dial-peer voice 1 pots
router(config-dial-peer)# volume 4
router(config-dial-peer)# dial-peer voice 2 pots
router(config-dial-peer)# volume 2
```

## Volume Adjustment Configuration Output Example

The following is an example of the volume adjustment configuration output from the **show running-config** command:

```
dial-peer voice 1 pots
destination-pattern 5551111
port 1
no call-waiting
ring 0
volume 4

dial-peer voice 2 pots
destination-pattern 5552222
port 2
no call-waiting
ring 0
volume 2
```

# Distinctive Ringing Based on Caller ID

The distinctive ringing feature enables you to configure the ring cadence for incoming calls based on the caller ID. You can choose from three ring cadences to associate with each telephone number and store up to twenty numbers per dial peer. You can configure a total of six dial peers but only one dial peer per port can be active at one time.

**Note** The distinctive ringing feature does not require subscription to any special service on the ISDN switch. However, if the Nariwake subscription is already active, then Nariwake takes precedence over this feature.

## Configuring Distinctive Ringing Based on Caller ID

To enable and configure distinctive ringing based on caller ID, use the following Cisco IOS command in dial-peer configuration mode:

**caller** *number* **ring** *cadence*

**no caller** *number* **ring** *cadence*

where *number* is the caller ID number of the incoming call, and *cadence* is the setting for ring cadence and duration. By default, this feature is disabled.

If you have configured the maximum number of twenty per dial peer, disable the numbers by using the **no caller** *number* **ring** *cadence* command.

Table 6-13 shows the available ring cadence settings.

***Table 6-13 Ring Cadence Settings***

| Cadence | Description |
|---|---|
| 1 | 1 sec on, 2 sec off (NTT defined regular ring) |
| 2 | 0.25 sec on, 0.2 sec off, 0.25 sec on, 2.3 sec off (NTT defined non-regular ring) |
| 3 | 0.5 sec on, 0.25 sec off, 0.25 sec on, 2 sec off (Cisco defined non-regular ring) |

## Distinctive Ringing Scenarios

Table 6-14 shows scenarios for distinctive ringing.

*Table 6-14 Scenarios for Distinctive Ringing*

| Condition | Event | Result |
|---|---|---|
| ISDN line is provisioned with Nariwake service. The user sets the same caller ID number that is set for Nariwake to distinctive ringing supported locally at the router. | An incoming voice call comes from the configured caller ID for POTS 1 or POTS 2. | The Nariwake service takes precedence over distinctive ringing based on caller ID.<br>The user at POTS 1 or POTS 2 hears the same ring cadence as that of the Nariwake service. |
| User configures distinctive ringing for POTS 1 or POTS 2, based on caller ID supported locally by the router. The user also sets the country group, which has a different ring cadence. | An incoming voice call comes from the caller ID number configured for POTS 1 or POTS 2. | Distinctive ringing takes precedence over the ring cadence set by the **pots country group** command.<br>The incoming call rings at POTS 1 or POTS 2 with the ring cadence specified in distinctive ringing based on caller ID. |
| User configures distinctive ringing based on caller ID supported locally by the router for POTS 1 or POTS 2. The user also configures a different ring cadence for the port by entering the **ring** command. | An incoming voice call comes from that caller ID number configured for POTS 1 or POTS 2. | Distinctive ringing based on caller ID takes precedence over the ring cadence set by the **ring** command.<br>The incoming call rings at POTS 1 or POTS 2 with the ring cadence specified in the distinctive ringing based on caller ID. |

## Distinctive Ringing Configuration Example

The following is an example of the distinctive ringing configuration:

```
cisco801# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
cisco801#(config)#dial-peer voice 1 pots
cisco801#(config-dial-peer)#caller-number 11111 ring 1
cisco801#(config-dial-peer)#caller-number 22222 ring 2
cisco801#(config-dial-peer)#caller-number 33333 ring 1
```

## Distinctive Ringing Configuration Output Example

The following is an example of the output for the distinctive ringing feature from the **show running-config** command:

```
!

dial-peer voice 1 pots
  no caller-id
  no forward-to-unused-port
  call-waiting
  ring 0
  no silent-fax
  registered-caller ring 1
  port 1
  volume 3
  caller-number 11111 ring 1
  caller-number 22222 ring 2
  caller-number 33333 ring 1
!
dial-peer voice 2 pots
  no caller-id
  no forward-to-unused-port
  call-waiting
  ring 0
  no silent-fax
  registered-caller ring 1
  port 1
  volume 3
  caller-number 11111 ring 1
  caller-number 33333 ring 1
  caller-number 22222 ring 2
```

# Subaddresses for POTS Ports

The subaddressing feature enables you to assign an ISDN subaddress to each POTS port so that an external call can be directly connected to the number dialed.

## Configuring Subaddresses for POTS Ports

To configure the subaddress for a POTS port, use the Cisco IOS **subaddress** command in dial-peer configuration mode:

```
subaddress number
```

```
no subaddress number
```

where *number* is the subaddress of a POTS port. Only one subaddress can be configured for each port. By default, no subaddresses are configured.

## Subaddressing Scenarios

Table 6-15 shows scenarios for subaddresses for a POTS port.

*Table 6-15 Subaddress Scenarios*

| Condition | Event | Result |
|---|---|---|
| User configures a destination pattern and a subaddress in a POTS 1 or POTS 2 dial peer. | An external voice call comes in with a called number and subaddress to the router. | The router accepts the incoming call and routes it to POTS or POTS 2 if the called number matches the destination pattern configured for the POTS dial peer. |
| User configures a destination pattern and subaddress in a POTS 1 or POTS 2 dial peer. | An external voice call comes in with a subaddress to the router but without a called number. | The router accepts the incoming call and routes it to POTS 1 or POTS 2 if the subaddress matches the subaddress configured for the POTS dial peer. This happens in the case of a point-to-point ISDN line. |
| User configures only the subaddress in a POTS 1 or POTS 2 dial peer. | An external voice call comes in with a subaddress to the router. | The router accepts the incoming call and routes it to POTS 1 or POTS 2 if the subaddress matches the subaddress configured for the POTS dial peer. This happens in the case of a point-to-point ISDN line. |
| User configures only the destination pattern in a POTS 1 or POTS 2 dial peer and doesn’t configure a subaddress for any of the POTS ports. | An external voice call comes in with a called number and a subaddress to the router. | The router accepts the incoming call and routes it to POTS 1 or POTS 2 if the subaddress matches the subaddress configured for the POTS dial peer. |

## Subaddressing Configuration Example

The following is an example of the subaddresses configuration:

```
router# configure terminal
router(config)# dial-peer voice 1 pots
router(config-dial-peer)# destination-pattern 5551111
router(config)# dial-peer voice 2 pots
router(config-dial-peer)# destination-pattern 5552222
router(config-dial-peer)# subaddress 10
```

## Subaddressing Configuration Output Example

The following is an example of the output for configuring subaddresses of the POTS ports:

```
dial-peer voice 1 pots
destination-pattern 5551111
port 1
no call-waiting
ring 0
volume 4
caller 1112222 ring 3
caller 2223333 ring 1
caller 3334444 ring 1
subaddress 20

dial-peer voice 2 pots
destination-pattern 5552222
port 2
no call-waiting
ring 0
volume 2
caller 1111111 ring 1
caller 2223323 ring 2
caller 3213213 ring 3
caller 8552345 ring 1
caller 2223456 ring 2
caller 3214567 ring 2
subaddress 10
```

# Caller ID on the Cisco 813 Router

The correct information is as follows:

By default, the caller ID feature is disabled. To enable this feature, use the Cisco IOS **caller-id** command in the dial-peer configuration command mode.

```
caller-id
no caller-id
```

## Debug POTS Commands

Use the following commands to debug problems with caller ID configuration:

- **debug pots driver**
- **debug pots csm**

Use the following commands for problems configuring other supplementary telephone features:

- **debug pots csm**
- **debug isdn event**
- **debug isdn q931**

For more information about using debug commands, refer to the Cisco IOS documentation.

# Local Call Forwarding

The local call forwarding feature enables you to forward an incoming voice call to an external telephone number if that call is not answered within a certain number of ring cycles. Highlights of this feature are as follows:

- If the telephone is picked up at the forwarded destination, the router connects the incoming call to the new destination.
- If the forwarded destination does not pick up the call within the timeout period, the router disconnects the call.
- If either party hangs up after a successful connection, the router disconnects the call.

**Note** The call forwarding feature uses the B channels to forward the voice call and to connect the caller and the forwarded destination. If one or both B channels are busy with data calls, the incoming voice call supersedes the data calls.

## Configuring Local Call Forwarding

To configure local call forwarding on your router, use the following Cisco IOS command in dial-peer configuration mode:

```
forward number after number of rings
no forward number after number of rings
```

where *number* is the external telephone number to forward an incoming voice call, and *number of rings* is the maximum number of ring cycles (from 0 to 7) before the router forwards the call. By default, this feature is disabled.

## Local Call Forwarding Scenarios

Table 6-16 shows scenarios for local call forwarding:

*Table 6-16 Scenarios for Local Call Forwarding*

| Condition | B1 Channel | B2 Channel | Event | Result |
|---|---|---|---|---|
| The feature is enabled through the command-line interface. | Free. | Free. | An external voice call comes in to POTS 1 or POTS 2. | The call is forwarded to the external destination number specified, and both B channels are busy with call forwarding. If the forwarded destination is busy, the router sends a disconnect signal to the incoming call. |

*Table 6-16 Scenarios for Local Call Forwarding (continued)*

| Condition | B1 Channel | B2 Channel | Event | Result |
|---|---|---|---|---|
| The feature is enabled through the command-line interface. | Data call in progress. | Data call in progress. | An external voice call comes in to POTS 1 or POTS 2. | The router waits for the specified number of rings and then bumps a data call to make a call to the forwarding destination. If the forwarded destination responds with a connect, then the router bumps the second data call and connects to the incoming call. The external caller and the forwarded destination will be able to converse. If the forwarding destination is busy, the router sends a disconnect to the incoming external call and the second data call is not bumped. |
| The feature is enabled through the command-line interface. | Data call in progress. | Free. | An external voice call comes in to POTS 1 or POTS 2. | The router waits for the specified number of rings and then makes a call to the forwarding destination. If the forwarded destination responds with a connect, the router bumps the data call and connects to the external incoming call. Now the external caller and the forwarded destination will be able to converse. If the forwarding destination is busy, the router sends a disconnect to the incoming call and the existing data call is not bumped. |
| The feature is enabled through the command-line interface. | Voice call in progress. | Voice call in progress. | An external voice call comes in to POTS 1 or POTS 2. | The router waits for the specified number of rings and then verifies that both the B channels are free. If the voice call from POTS 1 or POTS 2 is active, the router sends a disconnect signal to the incoming call. |

***Table 6-16 Scenarios for Local Call Forwarding (continued)***

| Condition | B1 Channel | B2 Channel | Event | Result |
|---|---|---|---|---|
| The feature is not enabled. | Local call forwarding is on. | Local call forwarding is on. | An external voice call comes in to POTS 1 or POTS 2. | Call waiting is not supported in this case. The router sends a disconnect signal to the incoming voice call.The caller hears a busy tone. |
| The feature is not enabled. | Local call forwarding is on. | Local call forwarding is on. | The user at POTS 1 or POTS 2 makes an outgoing call. | The user at POTS 1 or POTS 2 cannot make an external call. |

## Local Call Forwarding Configuration Example

The following is an example of configuring the local call forwarding feature:

```
router# configure terminal
router(config)# dial-peer voice 1 pots
router(config-dial-peer)# forward 8765432 after 0
router(config)# dial-peer voice 2 pots
router(config-dial-peer)# forward 1234567 after 3
```

## Local Call Forwarding Configuration Output Example

The following is an example of the output for local call forwarding configuration:

```
dial-peer voice 1 pots
destination-pattern 5551111
port 1
no call-waiting
ring 0
volume 4
caller 1112222 ring 3
caller 2223333 ring 1
caller 3334444 ring 1
subaddress 20
forward 8765432 after 0

dial-peer voice 2 pots
destination-pattern 5552222
port 2
no call-waiting
```

```
ring 0
volume 2
caller 1111111 ring 1
caller 2223323 ring 2
caller 3213213 ring 3
caller 8552345ring 1
caller 2223456 ring 2
caller 3214567 ring 2
subaddress 10
forward 1234567 after 3
```

# Support for PIAFS

Personal Handy-Phone System (PHS) Internet Access Forum Standard (PIAFS) is a standard error-correction protocol for cellular data communication that is designed to pass data over the Personal Handy-Phone System (PHS) of cellular system. It also provides transmission control procedures (comparable to OSI reference model layer 2) for high-quality data transmission. Both PIAFS version 2.0 and version 2.1 are supported on the Cisco 800 series routers.

The following common applications are supported using PIAFS in PHS data communications:

- E-mail service

  This enables the user to send and receive e-mail messages. E-mail is a basic service of the PHS multimedia communications menu.

- Fax service

  This enable faxing of data stored in a Personal Digital Assistant (PDA).

- Internet access

  Internet access has influenced PHS in that many users want to be able to obtain necessary information in a timely manner when they are outdoors. It is also projected that PHS will be used extensively to form intranets for in-house communications by facilitating the expansion of office LAN access points.

- Photograph transmission service

  This service can be realized by transmitting the signals of a digital still camera directly or through the medium of a personal computer. This can be regarded as another variation of data transmission service that can use the PHS for transmission.

- Mobile office service

  The spread of groupware recently has led to frequent instances where groups share common data bases in carrying out or supporting the execution of collaborative work. There are demands to extend this collaborative environment even to outside locations through the use of mobile communications. This is made possible by the use of PHS data communications.

The Cisco 800 series routers will accept incoming PIAFS calls from a peer supporting PIAFS 2.2 and will behave as speed variable type 2 devices. The Cisco 800 series routers will not request speed change but will respond to the speed change requests from the peer. See Table 6-17 below.

*Table 6-17 PIAFS Protocol for Request and Response*

| PIAFS Peer Request Protocol (Data Link Initiation Side) | 800 PIAFS Subsystem Response Protocol (Data Link Reception Side) |
|---|---|
| Fixed speed | Fixed speed |
| Speed variable type 1 | Speed variable type 2 |
| Speed variable type 2 | Speed variable type 2 |
| Speed variable type 3 | Speed variable type 2 |

The table indicates that the Cisco 800 series routers will act only as a PIAFS speed variable type 2 device for all the peers supporting PIAFS 2.2.

## Configuring PIAFS

This feature is available by default in all images. It is enabled when the ISDN switch type is set to INS (NTT) and PPP encapsulation is configured on the ISDN interface.

## PIAFS Scenarios

Table 6-18 shows scenarios for PIAFS. The feature is activated when the ISDN switch type is set to INS(NTT) and PPP encapsulation is configured on the ISDN interface.

*Table 6-18 Scenarios for PIAFS*

| B1 Channel | B2 Channel | Event | Result |
|---|---|---|---|
| Free | Free | An incoming PIAFS call comes in to the router. | The router negotiates the data transmission protocol and accepts the PIAFS call. The PIAFS peer runs the PHS application. |
| Data or voice call in progress | Free | An incoming PIAFS call comes in to the router. | The router negotiates the data transmission protocol and accepts the PIAFS call. The PIAFS peer runs the PHS application. |
| Data or voice call in progress | Data or voice call in progress | An incoming PIAFS call comes in to the router. | The router does not bump a data or voice call for a PIAFS call, therefore does not accept the PIAFS call. |
| Free | Free | The router is handling a 64 kbps PIAFS call, with a current speed of 32 kbps. During the course of the call, the remote end requests a rate change to 64 kbps. | The router successfully changes the speed of the PIAFS call from 32 kbps to 64 kbps. |
| | | The router is handling a 64 kbps PIAFS call. During the course of the call, the remote end requests a rate change to 32 kbps. | The router successfully changes the speed of the PIAFS call from 64 kbps to 32 kbps. |

*Table 6-18 Scenarios for PIAFS (continued)*

| B1 Channel | B2 Channel | Event | Result |
|---|---|---|---|
| Free | Free | The router is handling a 64 kbps PIAFS 2.0 call. During handover, the new cell is not able to allocate two channels for maintaining 64 kbps, so it requests the router to decrease the speed of the PIAFS call from 64 kbps to 32 kbps. | Since PIAFS 2.0 supports only fixed rate PIAFS call, the router does not accept the PIAFS call. |
| | | The router is handling a 64 kbps PIAFS 2.1 call. During handover, the new cell is not able to allocate two channels for maintaining 64 kbps, so it requests the router to decrease the speed of the PIAFS call from 64 kbps to 32 kbps. | Since PIAFS 2.1 supports best effort connection, the speed of the current PIAFS call is successfully decreased from 64 kbps to 32 kbps. |
| Free | PIAFS call in progress | The router is handling a PIAFS 2.0 call with the caller supporting PIAFS 2.0. A new PIAFS call comes from a caller supporting PIAFS 2.1 | The router simultaneously handles both PIAFS 2.0 and 2.1 calls. |
| | | The router is handling a PIAFS 2.1 call with the caller supporting PIAFS 2.1. A new PIAFS call comes from a caller supporting PIAFS 2.0 | The router simultaneously handles both PIAFS 2.0 and 2.1 calls. |

## PIAFS Status

The status of the PIAFS calls on the router can be checked by using the following command in privileged mode:

```
show piafs status
```

## PIAFS Configuration Output Example

The following is an example of the output for PIAFS configuration:

```
Number of active calls = 1
Details of connection 0
Call Direction is - INCOMING
    The speed is - 32K
    The Bchan assigned for this call is - B1 CHAN
    V42 Negotiated - YES
    V42 Parameters
        Direction - BOTH
        No of code words - 4096
        Max string length - 250
    First PPP Frame Detected - YES
    Piafs main FSM state - PIAFS_DATA
```

# Router Feature Configuration

This chapter includes basic feature-by-feature configuration procedures for Cisco 800 series and Cisco SOHO series routers. This chapter is useful if you have a network in place and you want to add specific features.

**Note** Every feature described is not necessarily supported on every router model. Where possible and applicable, feature limitations are listed.

If you prefer to use network scenarios to build a network, see Chapter 4, "Network Scenarios."

This chapter contains the following sections:

- Before You Configure Your Network, page 7-2
- Configuring Basic Parameters, page 7-3
- Configuring Bridging, page 7-14
- Configuring Static Routing, page 7-17
- Configuring Dynamic Routing, page 7-18
- Configuring IP EIGRP, page 7-20
- Configuring Addressing Parameters, page 7-22
- Configuring DHCP, page 7-27
- Configuring TACACS+, page 7-33
- Configuring an Extended Access List, page 7-34
- Configuring Quality of Service Parameters, page 7-36

- Configuring a Single-PVC Environment Using RFC 1483 Encapsulation, page 7-40
- Configuring Dial Backup, page 7-53
- Configuring IGMP Proxy and Sparse Mode, page 7-60
- Configuring IP Security and GRE Tunneling, page 7-63
- Configuring Multilink PPP Fragmentation and Interleaving, page 7-70
- Configuring Voice, page 7-73
- Cisco 827 Router Configuration Examples, page 7-78
- Corporate or Endpoint Router Configuration for Data and Voice Network, page 7-83

Each section includes a configuration example and verification steps, where available.

# Before You Configure Your Network

Before you configure your network, you must do the following:

- If applicable, order an ADSL, G.SHDSL, or ISDN line from your telephone service provider.
- Determine the number of PVCs that your service provider is giving you, together with their virtual path identifiers (VPIs) and virtual channel identifiers (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. In the case of routed RFC 1483, the service provider has to provide you with a static IP address. In the case of bridged RFC 1483, you may use DHCP to obtain your IP address or you may be given a static IP address from your service provider.
  - AAL5MUX PPP: With this type, you need to determine PPP-related configuration items.

- If you are setting up an Internet connection, gather the following information:
  - Point-to-Point Protocol (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 Internet Service Provider (ISP) account.
  - DNS server IP address and default gateways.
- If you are setting up a connection to a corporate network, you and its 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.

# Configuring Basic Parameters

To configure the router, perform the tasks described in the following sections:

- Configuring Global Parameters
- Configuring the Ethernet Interface
- Configuring the Dialer Interface
- Configuring the Loopback Interface
- Configuring the Asynchronous Transfer Mode Interface
- Configuring Command-Line Access to the Router

A configuration file example that illustrates how to configure the network is presented after the tasks.

After your router boots, the following prompt displays. Enter **no**.

```
Would you like to enter the initial configuration dialog [yes]: no
```

For complete information on how to access global configuration mode, see the "Entering Global Configuration Mode" section on page A-8. For more information on the commands used in the following tables, refer to the Cisco IOS Release 12.0 documentation set.

## Configuring Global Parameters

Follow the steps below to configure the router for global parameters.

| | Command | Task |
|---|---|---|
| Step 1 | **configure terminal** | Enter configuration mode. |
| Step 2 | **hostname** *name* | Specify the name for the router. |
| Step 3 | **enable secret** *password* | Specify an encrypted password to prevent unauthorized access to the router. |
| Step 4 | **ip subnet-zero** | Configure the router to recognize zero subnet range as valid range of addresses. |
| Step 5 | **no ip domain-lookup** | Disable the router from translating unfamiliar words (typos) entered during a console session into IP addresses. |

For complete information on the global parameter commands, refer to the Cisco IOS Release 12.0 documentation set.

## Configuring the Ethernet Interface

Follow the steps below to configure the Ethernet interface, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **interface ethernet 0** | Enter configuration mode for the Ethernet interface. |
| Step 2 | **ip address** *ip-address mask* | Set the IP address and subnet mask for the Ethernet interface. |

| | Command | Task |
|---|---|---|
| **Step 3** | **no shutdown** | Enable the Ethernet interface to change the state from administratively down to up. |
| **Step 4** | **exit** | Exit configuration mode for the Ethernet interface. |

For complete information on the Ethernet commands, refer to the Cisco IOS Release 12.0 documentation set. For more general information on Ethernet concepts, see Chapter 1, “Concepts.”

## Configuration Example

The following example shows the Ethernet interface configuration. You do not need to enter the commands marked “default.” These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

```
!
interface Ethernet0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast (default)
!
```

## Verifying Your Configuration

To verify that you have properly configured the Ethernet interface, enter the **show interface ethernet0** command. You should see a verification output like the example shown below.

```
router#sh int eth0
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)
```

# Configuring the Dialer Interface

Use these commands if you are using PPP encapsulation for the ATM PVC.

Follow the steps below to configure the dialer interface, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **interface dialer** *number* | Enter configuration mode for the dialer interface. |
| Step 2 | **encapsulation** *ppp* | Specify the encapsulation type for the PVC as PPP. |
| Step 3 | **ip address** *ip-address mask* | Set the IP address and subnet mask for the dialer interface. |
| Step 4 | **dialer pool** *number* | Specify which dialer pool number you are using. |
| Step 5 | **pvc** *vpi/vci* | Create an ATM PVC for each end node with which the router communicates. |
| Step 6 | **encapsulation aal5mux ppp dialer** | Specify the encapsulation type as AAL5MUX PPP. |
| Step 7 | **dialer pool-member** *number* | Specify a dialer pool-member. |
| Step 8 | **dialer-group** *number* | Specify a dialer group. The dialer group is required to fast-switch outgoing packets. |
| Step 9 | **exit** | Exit configuration mode for the ATM interface. |

## Configuration Example

The following example shows the dialer interface configuration. You do not need to input the commands marked “default.” These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

```
!
interface atm0
pvc 1/40
   encapsulation aal5mux ppp dialer
```

```
    dialer pool-member 1
!
interface dialer 0
ip address 200.200.100.1 255.255.255.0
encapsulation ppp
dialer pool 1
!
```

## Verifying Your Configuration

To verify that you have properly configured the dialer interface, enter the **show interface virtual-access 1** command. Both line protocol and dialer 0 should be up and running. You should see a verification output like the example shown below.

```
router(config-if)#sh int virtual-access 1
Virtual-Access1 is up, line protocol is up
    Hardware is Virtual Access interface
    Interface is unnumbered. Using address of Dialer0 (2.2.2.1)
    MTU 1500 bytes, BW 100000 Kbit, DLY 100000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set
```

**Virtual-access 1 is up** means that the interface is up and running. If you see the output **Virtual-access 1 is down**, it means that the interface is “administratively down,” and the interface is configured with the shutdown command. To bring the interface up, you must enter the **no shutdown** command.

# Configuring the Loopback Interface

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

For complete information on the loopback commands, refer to the Cisco IOS Release 12.0 documentation set.

## Configuration Tasks

Follow the steps below to configure the loopback interface.

| | Command | Task |
|---|---|---|
| **Step 1** | interface Loopback 0 | Enter configuration mode for the loopback interface. |
| **Step 2** | **ip address** *ip-address mask* | Set the IP address and subnet mask for the loopback interface. |
| **Step 3** | ip nat outside | Set the interface to be connected to the outside network. |
| **Step 4** | exit | Exit configuration mode for the loopback interface. |

## Sample Configuration

The loopback interface in this sample configuration is used to support NAT on the virtual-template interface. This sample configuration shows the loopback interface configured on the 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 Loopback0
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 Your Configuration

To verify that you have properly configured the loopback interface, enter the **show interface loopback 0** command. You should see a verification output similar to the following example.

```
Router #sh int loopback 0
Loopback0 is up, line protocol is up
  Hardware is Loopback
  Internet address is 200.200.100.1/24
  MTU 1514 bytes, BW 8000000 Kbit, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation LOOPBACK, loopback not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Another way to verify the loopback interface is to send multiple ping packets to 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 the Asynchronous Transfer Mode Interface

Use the following steps to configure the Asynchronous Transfer Mode (ATM) interface, beginning in global configuration mode.

**Note** The default service class for configuring the ATM interface is unspecified bit rate (ubr). You can change the service class to variable bit rate non-real time (vbr-nrt) or variable bit rate real time (vbr-rt) by using one of these commands: **vbr-nrt** or **vbr-rt**. Refer to the Cisco IOS Release 12.0 documentation set. For more information on definitions of service classes, see Chapter 1, "Concepts."

| | Command | Task |
|---|---|---|
| Step 1 | **interface ATM 0** | Enter configuration mode for the ATM interface. |
| Step 2 | **dsl equipment-type** {**co** \| **cpe**} | Configure the DSL equipment type, if applicable. |
| Step 3 | **dsl linerate** {*number* \| **auto**} | Specify the G.SHDSL line rate, if applicable. The range of valid numbers is between 72 and 2312. |
| Step 4 | **dsl operating-mode gshdsl symmetric annex** *annex* | Set the G.SHDSL operating mode, if applicable, and select the G.991.2 annex. |
| Step 5 | **ip address** *ip-address mask* | Set the IP address and subnet mask for the ATM interface. |
| Step 6 | **pvc** *vpi/vci* | Create an ATM PVC for each end node with which the router communicates. |
| Step 7 | **protocol ip** *ip-address* **broadcast** | Set the protocol broadcast for the IP address. |
| Step 8 | **encapsulation** *protocol* | Specify the encapsulation type for the PVC. Encapsulations can be specified as AAL5SNAP, AAL5MUX IP, or AAL5MUX PPP.[1] |
| Step 9 | **tx-ring-limit** *number* | Configure the size of the PVC transmit queue. The default setting is 6. |
| Step 10 | **no shutdown** | Enable the ATM interface. |
| Step 11 | **exit** | Exit configuration mode for the ATM interface. |

[1] This step is optional. If you specify the AAL5MUX PPP encapsulation, you will need to add an additional step to specify the dialer pool-member number using the command **dialer-pool member** number.

For complete information on the ATM commands, refer to the Cisco IOS Release 12.0 documentation set. For more general information on ATM concepts, see Chapter 1, “Concepts.”

## AAL5SNAP Encapsulation Configuration Example

The following example shows the ATM interface configuration for AAL5SNAP encapsulation.

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

```
!
interface ATM0
ip address 200.200.100.1 255.255.255.0
no ip directed-broadcast (default)
no atm ilmi-keepalive (default)
pvc 8/35
encapsulation aal5snap
protocol ip 200.200.100.254 broadcast
!
```

## Verifying Your Configuration

To verify that you have properly configured the ATM interface with AAL5SNAP encapsulation, enter the **show interface atm0** command. You should see a verification output like the example shown below.

```
router#sh int atm0
ATM0 is up, line protocol is up
    Hardware is PQUICC_SAR (with Alcatel ADSL Module)
Internet address is 1.1.1.1/24
MTU 1500 bytes, sub MTU 1500, BW 640 Kbit, DLY 80 usec, reliability
        113/255. txload 1/255, rxload 1/255
    Encapsulation aal5snap, loopback not set
    Keepalive not supported
DTR is pulsed for 5 seconds on reset
LCP Closed
```

## AAL5MUX PPP Encapsulation Configuration Example

The following example shows an ATM interface configuration for an AAL5MUX PPP encapsulation.

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

```
!
interface ATM0
no ip directed-broadcast (default)
no atm ilmi-keepalive (default)
pvc 8/35
encapsulation aal5mux ppp dialer
dialer pool-member 1
!
```

## Verifying Your Configuration

To verify that you have properly configured the ATM interface with AAL5MUX PPP encapsulation, enter the **virtual-access 1** command. You should see a verification output like the example shown below.

```
router#sh int virtual-access 1
Virtual-Access1 is up, line protocol is up
    Hardware is Virtual Access interface
    Interface is unnumbered. Using address of Dialer0 (2.2.2.1)
    MTU 1500 bytes, BW 100000 Kbit, DLY 100000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set
```

**Virtual-access 1 is up** means that the interface is up and running. If you see the output **Virtual-access 1 is down**, it means that the interface is “administratively down,” and the interface is configured with the shutdown command. To bring the interface up, you must enter the **no shutdown** command.

# Configuring Command-Line Access to the Router

Follow the steps below to configure parameters to control access to the router, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **line console 0** | Enter line configuration mode, and specify the console terminal line. |
| Step 2 | **password** *password* | Specify a unique password on the line. |
| Step 3 | **login** | Enable password checking at the terminal session login. |
| Step 4 | **exec-timeout 10 0** | Set the interval that the privileged EXEC command interpreter waits until user input is detected. Exec-timeout 10 0 is the default. |
| Step 5 | **line vty 0 4** | Specify a virtual terminal for remote console access. |
| Step 6 | **password** *password* | Specify a unique password on the line. |
| Step 7 | **login** | Enable password checking at virtual terminal session login. |
| Step 8 | **end** | Exit line configuration mode, and return to privileged EXEC mode. |

For complete information on the command line commands, refer to the Cisco IOS Release 12.0 documentation set.

## Configuration 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 that is 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 Bridging

Bridges are store-and-forward devices that use unique hardware addresses to filter traffic that would otherwise travel from one segment to another. You can configure the routers as pure bridges.

Follow the steps below to configure bridging, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **no ip routing** | Disable IP routing. |
| Step 2 | **bridge** *number* **protocol** *protocol* | Specify the bridge protocol to define the type of Spanning-Tree Protocol (STP). |
| Step 3 | **interface ethernet 0** | Enter configuration mode for the Ethernet interface. |
| Step 4 | **bridge-group** *number* | Specify the bridge-group number to which the Ethernet interface belongs. |
| Step 5 | **no shutdown** | Enable the Ethernet interface. |
| Step 6 | **exit** | Exit configuration mode for the Ethernet interface and the router. |
| Step 7 | **interface ATM 0** | Enter configuration mode for the ATM interface. |
| Step 8 | **dsl equipment-type** {**co** \| **cpe**} | Configure the DSL equipment type, if applicable. |
| Step 9 | **dsl linerate** {*number* \| **auto**} | Specify the G.SHDSL line rate, if applicable. The range of valid numbers is between 72 and 2312. |

| | Command | Task |
|---|---|---|
| Step 10 | **dsl operating-mode gshdsl symmetric annex** *annex* | Set the G.SHDSL operating mode, if applicable, and select the G.991.2 annex. |
| Step 11 | **pvc** *vpi/vci* | Create an ATM PVC for each end node with which the router communicates. |
| Step 12 | **encapsulation** *type* | Specify the encapsulation type for the PVC. |
| Step 13 | **bridge-group** *number* | Specify the bridge-group number to which the ATM interface belongs. |
| Step 14 | **no shutdown** | Enable the ATM interface. |
| Step 15 | **end** | Exit the configuration mode for the ATM interface. |

For complete information on the bridging commands, refer to the Cisco IOS Release 12.0 documentation set. For more general concepts on bridging, see Chapter 1, "Concepts."

# Configuration Example

The following configuration example uses bridging with AAL5SNAP encapsulation. You do not need to enter the commands marked "default." These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

This configuration example shows the Ethernet and ATM interfaces configured. The Ethernet interface has IP addressing turned off for bridging, and IP directed broadcast is disabled, which prevents the translation of directed broadcasts to physical broadcasts. The bridge-group number to which the ATM interface is associated is set to 1.

The ATM interface has a PVC of 8/35, and the encapsulation is set to AAL5SNAP. The IP address is disabled for bridging and the IP directed broadcast is disabled, which prevents the translation of directed broadcasts to physical broadcasts. The bridge protocol is set to 1 to define the STP.

```
no ip routing
!
interface Ethernet0
no ip address
no ip directed-broadcast (default)
```

```
bridge-group 1
!
interface ATM0
no ip address
no ip directed-broadcast (default)
pvc 8/35
encapsulation aal5snap
!
bridge-group 1
!
ip classless (default)
!
bridge 1 protocol ieee
!
end
```

# Verifying Your Configuration

To verify that you have properly configured bridging, enter the **show spanning-tree** command. You should see a verification output like the example shown below.

```
router#sh spanning-tree

Bridge group 1 is executing the IEEE compatible Spanning Tree protocol
    Bridge Identifier has priority 32768, address 1205.9356.0000
    Configured hello time 2, max age 20, forward delay 15
    We are the root of the spanning tree
    Port Number size is 9
    Topology change flag set, detected flag set
    Times: hold 1, topology change 35, notification 2
    hello 2, max age 20, forward delay 15
    Timers:hello 1, topology change 34, notification 0
    bridge aging time 15

Port 2 (Ethernet0) of Bridge group 1 is forwarding
    Port path cost 100, Port priority 128
    Designated root has priority 32768, address 1205.9356.0000
    Designated bridge has priority 32768, address 1205.9356.0000
    Designated port is 2, path cost 0
    Timers:message age 0, forward delay 0, hold 0
    BPDU:sent 0, received 0

Port 3 (ATM0 RFC 1483) of Bridge group 1 is forwarding
    Port path cost 1562, Port priority 128
```

```
Designated root has priority 32768, address 1205.9356.0000
Designated bridge has priority 32768, address 1205.9356.0000
Designated port is 3, path cost 0
Timers:message age 0, forward delay 0, hold 0
BPDU:sent 0, received 0
```

# Configuring Static Routing

Static routes are routing information that you manually configure into 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. Configuring static routing on the 800 series routers is optional.

Follow the steps below to configure static routing, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| **Step 1** | **ip classless** | Set up a best route for packets destined for networks unknown by the router. |
| **Step 2** | **ip route** *network-number mask* | Specify the static route for the IP packets. |
| **Step 3** | **end** | Exit router configuration mode. |

For complete information on the static routing commands, refer to the Cisco IOS Release 12.0 documentation set. For more general information on static routing, see Chapter 1, "Concepts."

# Configuration Example

In the following configuration example, the static route is sending all IP packets with a destination of 1.0.0.0 and a subnet mask of 255.0.0.0 out on the ATM interface to another device with an IP address of 14.0.0.1. Specifically, the packets are being sent to the configured PVC.

You do not need to enter the commands marked "default." These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

```
!
ip classless (default)
ip route 1.0.0.0 255.0.0.0 atm0 14.0.0.1
no ip http server (default)
!
```

## Verifying Your Configuration

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

You should see a verification output like the example shown below.

```
router#sh ip route
Codes:C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, 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 0.0.0.0 to network 0.0.0.0

5*  2.0.0.0/24 is subnetted, 1 subnets
C          2.2.2.0 is directly connected, Ethernet0/0
S* 0.0.0.0/0 is directly connected, Ethernet0/0
```

## Configuring Dynamic Routing

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

The IP routing protocol can use the Routing Information Protocol (RIP) or the Enhanced Interior Gateway Routing Protocol (EIGRP) to learn routes dynamically. You can configure either one of these routing protocols.

# Configuring RIP

Follow the steps below to configure RIP routing protocol on the router, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| **Step 1** | **router rip** | Enter router configuration mode and enable RIP on the router. |
| **Step 2** | **version 2** | Specify use of RIP version 2. |
| **Step 3** | **network** *network-number* | Specify the network number for each directly connected network. |
| **Step 4** | **no auto-summary** | Disable automatic summarization of subnet routes into network-level routes. This allows subprefix routing information to transmit across classful network boundries. |
| **Step 5** | **end** | Exit router configuration mode. |

For complete information on the dynamic routing commands, refer to the Cisco IOS Release 12.0 documentation set. For more general information on RIP, refer to Chapter 1, "Concepts."

## Configuration Example

The following configuration shows RIP version 2 enabled in IP network 10.10.10.0.

You do not need to enter the commands marked "default." These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

```
!
    router rip
    version 2
    network 10.0.0.0
    no auto-summary
!
```

## Verifying Your 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#sh ip route
Codes:C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, 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

     2.0.0.0/24 is subnetted, 1 subnets
C       2.2.2.0 is directly connected, Ethernet0/0
R    3.0.0.0/8 [120/1] via 2.2.2.1, 00:00:02, Ethernet0/0
```

# Configuring IP EIGRP

Follow the steps below to configure IP EIGRP, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **router eigrp** *autonomous-system* | Enter router configuration mode and enable EIGRP on the router. The autonomous-system number identifies the route to other EIGRP routers and is used to tag the EIGRP information. |
| Step 2 | **network** *network-number* | Specify the network number for each directly connected network. |
| Step 3 | **end** | Exit router configuration mode. |

For complete information on the IP EIGRP commands, refer to the Cisco IOS Release 12.0 documentation set. For more general information on EIGRP concepts, see Chapter 1, “Concepts.”

## Configuration Example

The following configuration shows EIGRP routing protocol enabled in IP networks 10.0.0.0 and 172.17.0.0. The EIGRP autonomous system number is assigned as 100.

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

```
!
router eigrp 100
   network 10.0.0.0
      network 172.17.0.0
!
```

## Verifying Your Configuration

To verify that you have properly configured IP EIGRP, enter the **show ip route** command and look for EIGRP routes signified by “D.” You should see a verification output like the following example.

```
router#sh ip route
Codes:C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, 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

       2.0.0.0/24 is subnetted, 1 subnets
C   2.2.2.0 is directly connected, Ethernet0/0
D    3.0.0.0/8 [90/409600] via 2.2.2.1, 00:00:02, Ethernet0/0
```

# Configuring Addressing Parameters

This section describes how to configure addressing using Network Address Translation (NAT) and Easy IP Phase 1 and 2.

## Configuring NAT

You can configure NAT for either static or dynamic address translations.

Follow the steps below to configure static or dynamic inside source translation, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **ip nat pool** *name start-ip end-ip* {**netmask** *netmask* \| **prefix-length** *prefix-length*} | Create pool of global IP addresses for NAT. |
| Step 2 | **access-list** *access-list-number* **permit** *source* [*source-wildcard*] | Define a standard access list permitting addresses that need translation. |
| Step 3 | **ip nat inside source list** *access-list-number* **pool** *name* | Enable dynamic translation of addresses permitted by access list to one of addresses specified in pool. |
| Step 4 | **ip nat inside source static** *local-ip global-ip number* **extendable** | Enable static translation of specified inside local address to globally unique IP address. This command is optional. |
| Step 5 | **interface ethernet 0** | Enter configuration mode for the Ethernet interface. |
| Step 6 | **ip nat inside** | Establish the Ethernet interface as the inside interface. |
| Step 7 | **exit** | Exit configuration mode for the Ethernet interface. |
| Step 8 | **interface atm 0** | Enter configuration mode for the ATM interface. |
| Step 9 | **dsl equipment-type** {**co** \| **cpe**} | Configure the DSL equipment type, if applicable. |

| | Command | Task |
|---|---|---|
| **Step 10** | **dsl linerate** {*number* \| **auto**} | Specify the G.SHDSL line rate, if applicable. The range of valid numbers is between 72 and 2312. |
| **Step 11** | **dsl operating-mode gshdsl symmetric annex** *annex* | Set the G.SHDSL operating mode, if applicable, and select the G.991.2 annex. |
| **Step 12** | **ip nat outside** | Establish the ATM interface as the outside interface. |
| **Step 13** | **exit** | Exit configuration mode for the ATM interface. |

**Note** If you want to use NAT with a virtual template interface, you must configure a loopback interface.

For complete information on the NAT commands, refer to the Cisco IOS Release 12.0 documentation set. For general information on NAT concepts, see Chapter 1, "Concepts."

## Configuration Example

The following configuration shows NAT configured for the Ethernet and ATM interfaces.

The Ethernet 0 interface has an IP address of 192.168.1.1 with a subnet mask of 255.255.255.0. NAT is configured for *inside*, which means that the interface is connected to the inside network that is subject to NAT translation.

The ATM 0 interface has an IP address of 200.200.100.1 and a subnet mask of 255.255.255.0. NAT is configured for *outside*, which means that the interface is connected to an outside network, such as the Internet.

You do not need to enter the commands marked "default." These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

```
!
interface Ethernet0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast (default)
```

```
ip nat inside
!
interface ATM0
ip address 200.200.100.1 255.255.255.0
no ip directed-broadcast (default)
ip nat outside
no atm ilmi-keepalive (default)
pvc 8/35
encapsulation aal5snap
!
ip route 0.0.0.0.0.0.0.0 200.200.100.254
!
ip nat pool test 200.200.100.1 200.200.100.1 netmask 255.255.255.0
ip nat inside source list 101 pool test overload
ip classless (default)
!
```

## Verifying Your Configuration

To verify that you have properly configured NAT, enter the **show ip nat statistics** command. You should see a verification output like the example shown below.

```
router#sh ip nat statistics
Total active translations:45 (10 static, 35 dynamic; 45 extended)
Outside interfaces:
  ATM0
Inside interfaces:
  Ethernet0
Hits:34897598  Misses:44367
Expired translations:119305
Dynamic mappings:
-- Inside Source
access-list 1 pool homenet refcount 14
pool homenet:netmask 255.255.255.0
        start 200.200.100.1 end 200.200.100.1
        type generic, total addresses 1, allocated 1 (100%), misses
```

# Configuring Easy IP (Phase 1)

This section explains how to configure Easy IP (Phase 1). Easy IP Phase 1 includes NAT overload and PPP/Internet Protocol Control Protocol (IPCP). NAT overload means that you can use one registered IP address for the interface and use it to access the Internet from all devices in the network.

With PPP/IPCP, Cisco 800 series routers automatically negotiate a globally unique (registered or public) IP address for the interface from the ISP route.

Follow the steps below to configure Easy IP (Phase 1), beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **access-list** *access-list-number* **permit** *source* [*source-wildcard*] | Define a standard access list that permits nonregistered IP addresses of hosts. |
| Step 2 | **ip nat inside source list** *access-list-number* **interface** *interface* **overload** | Set up translation of addresses identified by the access list defined in Step 1. |
| Step 3 | **interface ethernet 0** | Enter configuration mode for the Ethernet interface. |
| Step 4 | **ip nat inside** | Establish the Ethernet interface as the inside interface for NAT. |
| Step 5 | **no shutdown** | Enable the Ethernet interface and the configuration changes just made to it. |
| Step 6 | **exit** | Exit configuration mode for the Ethernet interface. |
| Step 7 | **interface dialer** | Enter configuration mode for the dialer interface. |
| Step 8 | **ip address negotiated** | Assign a negotiated IP address to the dialer interface. |
| Step 9 | **ip nat outside** | Establish the dialer interface as the outside interface for NAT. |
| Step 10 | **dialer pool** *number* | Specify which dialer pool number you are using. |
| Step 11 | **exit** | Exit the dialer interface. |
| Step 12 | **interface ATM 0** | Enter configuration mode for the ATM interface. |
| Step 13 | **dsl equipment-type** {**co** \| **cpe**} | Configure the DSL equipment type, if applicable. |
| Step 14 | **dsl linerate** {*number* \| **auto**} | Specify the G.SHDSL line rate, if applicable. The range of valid numbers is between 72 and 2312. |

| | Command | Task |
|---|---|---|
| Step 15 | **dsl operating-mode gshdsl symmetric annex** *annex* | Set the G.SHDSL operating mode, if applicable, and select the G.991.2 annex. |
| Step 16 | **pvc** *vpi/vci* | Create an ATM PVC for each end node with which the router communicates. |
| Step 17 | **encapsulation aal5mux ppp dialer** | Specify the encapsulation type for the PVC to be AAL5MUX PPP and point back to the dialer interface. |
| Step 18 | **dialer pool-member** *number* | Specify which dialer pool-member you are using. |
| Step 19 | **no shutdown** | Enable the interface and configuration changes just made to the ATM interface. |
| Step 20 | **exit** | Exit configuration mode for the ATM interface. |

For complete information on the Easy IP commands, refer to the Cisco IOS Release 12.0 documentation set. For general information on Easy IP (Phase 1) concepts, see Chapter 1, “Concepts.”

# Configuring Easy IP (Phase 2)

This section explains how to configure a Cisco 800 series router as a DHCP server.

The Easy IP (Phase 2) feature combines DHCP server and relay. With DHCP, LAN devices on an IP network (DHCP clients) can request IP addresses from the DHCP server. The DHCP server allocates IP addresses from a central pool as needed. A DHCP server can be a workstation, PC, or a Cisco router. With the DHCP relay feature configured on the router, the routers can relay IP address requests from the LAN interface and to the DHCP server as shown in Figure 7-1 and Table 7-1.

*Figure 7-1 Easy IP (Phase 2)–DHCP Server and Relay*

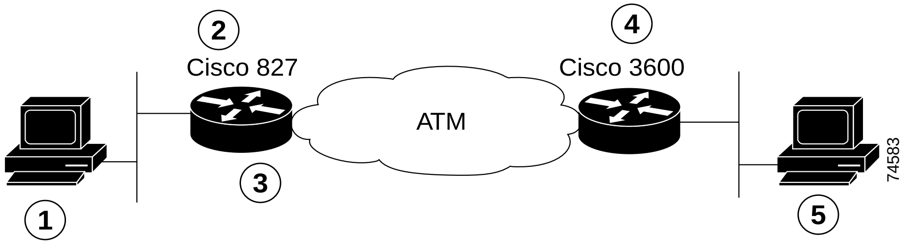


*Table 7-1 Key for Easy IP (Phase 2)–DHCP Server and Relay*

| Callout Number | Description |
|---|---|
| 1 | DHCP client |
| 2 | Remote office with Cisco 827 router |
| 3 | DHCP relay |
| 4 | Corporate office with Cisco 3600 router |
| 5 | DHCP server |

# Configuring DHCP

The following sections describe how to configure the router as a DHCP client, server, or relay.

## Configuring DHCP Client Support

Follow these steps to configure the router for DHCP client support:

**Step 1** Configure the BVI interface by entering the **ip address dhcp client-id Ethernet 0** command.

Specifying the value *client-id ethernet0* means that the MAC address of the Ethernet interface is used as the client ID when the DHCP request is sent. Otherwise, the MAC address of the BVI interface is used as the client ID.

**Step 2** Configure NAT:

a. Configure the BVI interface by entering the **ip nat outside** command.

b. Configure the Ethernet interface by entering the **ip nat inside** command.

c. Create an access list under NAT by entering the **access-list 1 permit** *ip address* command to match all Ethernet IP addresses.

d. Configure the source list under NAT by entering the **ip nat inside source list 1 interface BVI 1 overload** command.

**Step 3** Configure the Cisco router to act as a DHCP server. This step is optional.

a. At the `config-if` router prompt, enter the **ip dhcp pool** *server name* command.

b. Enter the **import all** command to have the Cisco router retrieve the Microsoft Windows nameserver (WINS) and domain name system (DNS) server addresses for name resolution.

## Configuration Example

The following example shows a configuration of the DHCP client.

```
Current configuration:
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname c827
!
!
ip subnet-zero
ip dhcp excluded-address 10.10.10.1
!
ip dhcp pool SERVER
 network 10.10.10.0 255.255.255.0
 default-router 10.10.10.1
 import all
!
bridge irb
interface Ethernet0
 ip address 10.10.10.1 255.255.255.0
 no ip directed-broadcast
 ip nat inside
!
interface ATM0
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
 bundle-enable
 hold-queue 208 in
!
interface ATM0.1 point-to-point
 no ip directed-broadcast
 pvc 1/100
 encapsulation aal5snap
!
bridge-group 1
!
interface ATM0.2 point-to-point
 ip address 5.0.0.2 255.0.0.0
 no ip directed-broadcast
 pvc 1/101
 protocol ip 5.0.0.1 broadcast
 protocol ip 5.0.0.5 broadcast
 encapsulation aal5snap
!
!
interface BVI1
 ip address dhcp client-id Ethernet0
 no ip directed-broadcast
 ip nat outside
!
ip nat inside source list 1 interface BVI1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 BVI1
no ip http server
!
access-list 1 permit 10.10.10.0 0.0.0.255
bridge 1 protocol ieee
bridge 1 route ip
!
voice-port 1
timing hookflash-in 0
```

```
!
voice-port 2
timing hookflash-in 0
!
voice-port 3
timing hookflash-in 0
!
voice-port 4
timing hookflash-in 0
!
!
line con 0
exec-timeout 0 0
transport input none
stopbits 1
line vty 0 4
password lab
login
!
scheduler max-task-time 5000
end
```

# Configuring DHCP Server

Follow the steps below to configure the router as a DHCP server, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **ip dhcp pool** *name* | Enter DHCP configuration mode, and create a pool of IP addresses that can be assigned to DHCP clients. |
| Step 2 | **network** *ip-address subnet-mask* | Specify a range of IP addresses that can be assigned to the DHCP clients. |
| Step 3 | **domain-name** *domain name* | Configure the domain name. |
| Step 4 | **dns-server** *ip-address* | Designate the router as the default router, and specify an IP address. |
| Step 5 | **netbios-name-server** *ip-address* | Configure the netbios name server. |
| Step 6 | **default-router** *ip-address* | Configure the DNS server. |

| | Command | Task |
|---|---|---|
| Step 7 | **lease** *days hours minutes* | Specify the duration of the lease. |
| Step 8 | **exit** | Exit DHCP configuration mode. |

For more information on the features not used in this configuration, refer to the *Cisco IOS DHCP Server* feature module. For more general information on DHCP servers, refer to Chapter 1, "Concepts."

## Configuration Example

The following configuration shows a DHCP server configuration for the IP address 20.1.1.2.

```
!
ip dhcp pool CLIENT
   network 20.20.20.0 255.255.255.0
   domain-name cisco.com
   default-router 20.20.20.20
   netbios-name-server 1.1.1.1
   dns-server 1.1.1.2
   lease 0 1
!
```

## Verifying Your Configuration

To verify that you have properly configured the DHCP server, enter the **show dhcp server** command and look for the assigned server IP. You should see a verification output like the example shown below.

```
router# sh dhcp server
show ip dhcp binding
show ip dhcp conflict
show ip dhcp server statics
```

# Configuring the DHCP Relay

This section describes how to configure the router to forward User Datagram Protocol (UDP) broadcasts, including IP address requests, from DHCP clients.

Follow the steps below to configure the DHCP relay, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **interface Ethernet 0** | Enter configuration mode for the Ethernet interface. |
| Step 2 | **ip helper-address** *address* | Forward default UDP broadcasts including IP configuration requests to the DHCP server. |
| Step 3 | **no shutdown** | Enable the Ethernet interface and the configuration changes. |
| Step 4 | **exit** | Exit configuration mode for the Ethernet interface. |

For complete information on the DHCP relay commands, refer to the Cisco IOS Release 12.0 documentation set. For more general information on DHCP relays, refer to Chapter 1, "Concepts."

## Configuration Example

The following configuration contains commands relevant to DHCP relay only.

You do not need to enter the commands marked "default." These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

```
!
int Ethernet0
ip address 192.168.100.1 255.255.255.0
ip helper-address 200.200.200.1
!
```

## Verifying Your Configuration

To verify that you have properly configured the DHCP relay, enter the **show dhcp server** command. You should see verification output like the example shown below.

```
router#sh dhcp server
   DHCP server:2.2.2.2
    Leases:  0
    Offers:  0      Requests:0     Acks:0     Naks:0
    Declines:0      Releases:0     Bad: 0
```

# Configuring TACACS+

The Cisco 806, 827, 831, 836, 837, 827H, and 827-4V routers and the Cisco SOHO 71, 91, 96, and 97 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.

To configure your router to support TACACS+, perform the following tasks:

| | Command | Task |
|---|---|---|
| **Step 1** | **aaa new-model** | Enter the global configuration command to enable AAA. AAA must be configured to use TACACS+. |
| **Step 2** | **tacacs-server host** | Specify the IP address of one or more TACACS+ daemons. |
| **Step 3** | **tacacs-server key** | Specify an encryption key that will be used to encrypt all exchanges between the network access server and the TACACS+ daemon. This same key must also be configured on the TACACS+ daemon. |

| | Command | Task |
|---|---|---|
| Step 4 | **aaa authentication** | Define the method lists that use TACACS+ for authentication. |
| Step 5 | **line** | Apply the defined method lists to various interfaces. |

You may need to perform other configuration steps to enable accounting for TACACS+ connections. For instructions on configuring TACACS+, refer to the *Security Configuration Guide*.

# Configuring an Extended Access List

Follow the steps below to include one or more extended access lists in your router configuration, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **access-list 100 permit tcp any ip** *ip address-mask* **established** | Permit any host on the network to access any Internet server. |
| Step 2 | **access-list 100 deny ip** *ip adddress-mask* **any** | Deny any Internet host from spoofing any host on the network. |
| Step 3 | **access-list 100 permit tcp host** *ip address-mask* | Permit Internet DNS server to send TCP replies to any host on the network. |
| Step 4 | **access-list 100 permit udp host** *ip address-mask* | Permit Internet DNS server to send UDP replies to any host on the network. |
| Step 5 | **access-list 100 permit tcp any host** *ip address* | Permit SMTP mail server to access any Internet server. |
| Step 6 | **access-list 100 permit tcp any host** *ip address* | Permit web server to access any Internet server. |
| Step 7 | **access-list 100 permit tcp any host** *ip address* | Permit FTP server to access any Internet server. |
| Step 8 | **access-list 100 deny tcp any** *ip address-mask* | Restrict any Internet host from making a Telnet connection to any host on the network. |

| | Command | Task |
|---|---|---|
| **Step 9** | **interface atm 0** | Enter configuration mode for the ATM interface. |
| **Step 10** | **dsl equipment-type** *co/cpe* | Configure the DSL equipment type, if applicable. |
| **Step 11** | **dsl linerate** *number/auto* | Specify the G.SHDSL line rate, if applicable. The range of valid numbers is between 72 and 2312. |
| **Step 12** | **dsl operating-mode gshdsl symmetric annex** *annex* | Set the G.SHDSL operating mode, if applicable, and select the G.991.2 annex. |
| **Step 13** | **ip access-group 100 in** | Activate access list 100. |
| **Step 14** | **no shutdown** | Enable the interface and configuration changes made to the interface. |
| **Step 15** | **exit** | Exit configuration mode for the ATM interface. |

For more complete information on the extended access list commands, refer to the Cisco IOS Release 12.0 documentation set. For information on TCP and UDP port assignments, see Appendix C, “Common Port Assignments.”

# Configuration Example

This configuration shows an access list being applied to IP address 192.168.1.0.

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

```
!
access-list 101 permit tcp any host 192.168.1.0 0.0.0.255
!
```

# Configuring Quality of Service Parameters

This section describes how to configure quality of service (QoS) parameters. The following are requirements for voice QoS:

- Priority queuing for voice traffic
- Fragmenting large data packets and interleaving voice packets

You can configure QoS in a single- or multiple-PVC environment. In a single-PVC environment, the traffic relies on IOS to provide priority queuing, using class-based weighted fair queuing (CBWFQ) to prioritize voice traffic and using MTU size reduction to perform Layer 3 fragmentation of data packets. In a multiple-PVC environment, the traffic relies on the ATM interface to provide priority queuing for voice and fragmentation and interleaving.

**Note** QoS parameters are supported only on routers with voice features.

For complete information on the QoS commands, refer to the Cisco IOS documentation set. For general information on QoS concepts, see Chapter 1, "Concepts."

## Configuring a Single-PVC Environment

In the single-PVC environment, the traffic relies on IOS to provide priority queuing (using CBWFQ). The tasks to configure a single-PVC environment are as follows:

- Configuring IP Precedence 5 for voice packets
- Configuring an access list and voice class
- Configuring a policy map and specify priority queuing for voice class
- Associating the policy map to the ATM PVC and decreasing the MTU of the ATM interface

## Configuring IP Precedence

IP Precedence gives voice packets a higher priority than other IP data traffic. The **ip precedence** command is used by the router to differentiate voice traffic from data traffic. Therefore, you need to ensure that the data IP packets do not have the same IP precedence as that of the voice packets.

Follow the steps below to configure real-time voice traffic precedence over other IP network traffic, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **dial-peer voice** *number* **voip** | Enter the dial peer configuration mode to configure a VoIP dial peer. |
| Step 2 | **destination-pattern** *number* | Set a destination pattern. |
| Step 3 | **session target** {**ipv4**:*destination-address*} | Specify a destination IP address for the dial peer. |
| Step 4 | **ip precedence** *number* | Select a precedence level for the voice traffic associated with that dial peer. |
| Step 5 | **exit** | Exit configuration mode for the dial peer interface. |

**Note** In IP Precedence, the numbers 1 through 5 identify classes for IP flows; the numbers 6 through 7 are used for network and backbone routing and updates. It is recommended that IP Precedence 5 is used for voice packets.

## Configuring an Access List and Voice Class

Follow the steps below to create a policy map and to associate a priority queue with the voice class, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **access-list 101 permit ip** *any any precedence 5* | Configure an access list to match voice packets. |

| | Command | Task |
|---|---|---|
| Step 2 | **class-map** *voice* | Configure a voice class. |
| Step 3 | **match access-group 101** | Associate the voice class with the access list. |

## Configuring a Policy Map and Specifing Voice Queuing

Follow the steps below to configure a policy map and to specify voice queuing, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **policy map *name*** | Configure a policy map.[1] |
| Step 2 | **class *voice*** | Specify the class for queuing. |
| Step 3 | **priority *number*** | Specify the priority for queuing. |

[1] Total bandwidth for the policy map may not exceed 75 percent of the total PVC bandwidth.

## Configuring a Policy Map and Specifying Priority Queuing for Voice Class

Follow the steps below to associate the policy map to the ATM PVC and decrease the MTU of the ATM interface so that large data packets are fragmented, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **policy map** *name* | Configure a policy map.[1] |
| Step 2 | **class** *voice* | Specify the class for queuing. |
| Step 3 | **priority** *bandwidth* | Specify the priority for queuing. |
| Step 4 | **exit** | Exit configuration mode for the policy map. |

[1] Total bandwidth for the policy map may not exceed 75 percent of the total PVC bandwidth.

## Associating the Policy Map to the ATM PVC and Decreasing the ATM Interface MTU

Use the following table to associate the policy map to the ATM PVC and decrease the MTU, beginning in global configuration mode. It is recommended that *300* is used for the MTU size because it is larger than the size of the voice packets generated by the different codecs.

**Note** The default service class for configuring the ATM interface is unspecified bit rate (ubr). In order to attach the policy map to the ATM PVC, you must use a service class of vbr-nrt or vbr-rt.

| | Command | Task |
|---|---|---|
| Step 1 | **interface ATM 0** | Enter configuration mode for the ATM interface. |
| Step 2 | **ip address** *ip-address mask* | Set the IP address and subnet mask for the ATM interface. |
| Step 3 | **pvc** *vpi/vci* | Create an ATM PVC for each end node with which the router communicates. |
| Step 4 | **encapsulation** *protocol* | Specify the encapsulation type for the PVC. Encapsulations can be specified as AAL5SNAP or AAL5MUX PPP. |
| Step 5 | **service policy out** *name* | Associate the service policy name. |
| Step 6 | **vbr-rt** *pcr scr bs* | Specify the service class. |
| Step 7 | **exit** | Exit configuration mode for the ATM PVC. |
| Step 8 | **mtu** *number* | Specify the MTU for the ATM interface. |
| Step 9 | **no shutdown** | Enable the ATM interface. |
| Step 10 | **exit** | Exit configuration mode for the ATM interface. |

## Configuration Example

The following example shows a voice QoS configuration in a single-PVC environment using AAL5SNAP encapsulation.

```
!
dial-peer voice 105 voip
destination-pattern 3..
session target ipv4:10.1.2.3
ip precedence 5

access-list 101 permit ip any any precedence critical

class-map voice
match access-group 101

policy-map mypolicy
class voice
priority 480

int atm0
mtu 300
pvc 8/35
encapsulation aal5snap
service-policy out mypolicy
vbr-rt 640 640 10
!
```

# Configuring a Single-PVC Environment Using RFC 1483 Encapsulation

This section describes configuring of a single-PVC environment using RFC 1483.

In a single-PVC environment using RFC 1483 encapsulation, the traffic relies on Cisco IOS to provide priority queuing using low latency queuing (LLQ). The following tasks are needed to configure a single-PVC environment:

- Differentiating Between Data and Voice Packets
- Configuring an Access List and Voice Class
- Configuring a Policy Map and Specifying Voice Queuing

- Associating the Policy Map with the ATM PVC and Using TCP MSS Adjust
- Fine-Tuning the Size of the PVC ATM Transmit Ring Buffer

## Differentiating Between Data and Voice Packets

To give priority to voice packets, the router must differentiate between the entering voice and data packets. One way to differentiate the packets is to examine their source or destination IP addresses, because data and VoIP devices may have different IP addresses.

Another way to differentiate the packet is use IP Precedence. Usually, data packets have precedence 0, while voice packets have IP precedence 5. To learn how to configure the IP Precedence for voice packets, refer to the documentation for your VoIP device.

**Note** In IP Precedence, the numbers 1 through 5 identify classes for IP flows; the numbers 6 through 7 are used for network and backbone routing and updates. It is recommended that IP Precedence 5 be used for voice packets.

## Configuring an Access List and Voice Class

Assuming that all voice packets have precedence 5 and that all data packets have precedence 0, perform these steps to configure an access-list that matches all precedence 5 packets, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| **Step 1** | **access-list 101 permit ip** *any any precedence* | Configure an access list to match voice packets. |
| **Step 2** | **class-map** *voice* | Configure a voice class |
| **Step 3** | **match access-group 101** | Associate the voice class with the access list. |

## Configuring a Policy Map and Specifying Voice Queuing

Follow the steps below to configure a policy may and to specify voice queuing, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **policy map** *name* | Configure a policy map.[1] |
| Step 2 | **class** *voice* | Specify the class for queuing. |
| Step 3 | **priority** *bandwidth* | Specify the bandwidth for this strict priority queue. |

[1] Total bandwidth for the policy map may not exceed 75 percent of the total PVC bandwidth.

## Associating the Policy Map with the ATM PVC and Using TCP MSS Adjust

Perform the steps below to associate the policy map with the ATM PVC and to use the **TCP MSS adjust** command to control delay, beginning in global configuration mode.

**Note** The default service class for configuring the ATM interface is unspecified bit rate (ubr). To attach the policy map to the ATM PVC, you must use a service class of vbr (nrt) or vbr (rt).

| | Command | Task |
|---|---|---|
| Step 1 | **interface ATM 0** | Enter configuration mode for the ATM interface. |
| Step 2 | **dsl equipment-type** {**co** \| **cpe**} | Configure the DSL equipment type. |
| Step 3 | **dsl linerate** {*number*\| **auto**} | Specify the ADSL line rate. The range of valid numbers is between 72 and 2312. |
| Step 4 | **ip address** *ip-address mask* | Set the IP address and subnet mask for the ATM interface. |

| | Command | Task |
|---|---|---|
| Step 5 | **pvc** *vpi/vci* | Create an ATM PVC for each end node with which the router communicates. |
| Step 6 | **encapsulation** *protocol* | Specify the encapsulation type for the PVC. Encapsulations can be specified as either AAL5SNAP or AAL5MUX PPP. |
| Step 7 | **service policy out** *name* | Associate the service policy name. |
| Step 8 | **vbr-rt** *pcr scr bs* | Specify the service class. |
| Step 9 | **exit** | Exit configuration mode for the ATM PVC. |
| Step 10 | **ip tcp adjust-mss** *mss* | Specify the TCP maximum segment size (MSS). |
| Step 11 | **no shutdown** | Enable the ATM interface. |
| Step 12 | **exit** | Exit configuration mode for the ATM interface. |

# Fine-Tuning the Size of the PVC ATM Transmit Ring Buffer

Each PVC has a hardware output first-in first-out (FIFO) queue that temporarily stores packets before they are sent out to the transceiver. In order to reduce latency for voice packets, you may need to reduce the size of this queue. Reducing the queue size reduces the maximum number of data packets that are “ahead” of a voice packet in the transmit queue. However, a transmit queue size that is too small may affect transmit throughput performance.

# Configuration Example

The following example shows a voice QoS configuration in a single-PVC environment using AAL5SNAP encapsulation.

```
access-list 101 permit ip any any precedence critical

class-map voice
match access-group 101

policy-map mypolicy
class voice
```

```
priority 480

int atm0
   dsl equipment-type CPE
   dsl linerate AUTO
ip tcp-mss 1452
pvc 8/35
encapsulation aaal5snap
service-policy out mypolicy
vbr-rt 1000 1000 1
tx-ring-limit 5
!
```

# Configuring a Single-PVC Environment Using PPP over ATM and Multilink Encapsulation

This section describes configuring of a single-PVC environment using PPP over ATM and multilink encapsulation.

The "Configuring Link Fragmentation and Interleaving with Low Latency Queuing" section on page 7-46 describes configuring multilink PPP fragmentation and interleaving for a second single-PVC environment.

In a single-PVC environment using PPP over ATM multilink encapsulation, the traffic relies on Cisco IOS to provide priority queuing using LLQ. These tasks are involved in configuring a single-PVC environment:

- Differentiating Between Data and Voice Packets
- Configuring the Policy Map and Specifying Voice Queuing
- Associating the Policy Map to the ATM PVC
- Configuring Link Fragmentation and Interleaving with Low Latency Queuing

## Differentiating Between Data and Voice Packets

To give priority to voice packets, the router must differentiate between the entering voice and data packets. One way to differentiate the packets is to examine the source or destination IP addresses, because data and VoIP devices may have different IP addresses.

Another way to differentiate the packets is use IP Precedence. Usually, data packets have precedence 0, while voice packets have IP precedence 5. To learn how to configure the IP precedence for voice packets, refer to the documentation for your VoIP device.

**Note** In IP Precedence, the numbers 1 through 5 identify classes for IP flows; the numbers 6 through 7 are used for network and backbone routing and updates. It is recommended that IP Precedence 5 be used for voice packets.

## Configuring the Policy Map and Specifying Voice Queuing

Follow the steps below to configure a policy may and to specify voice queuing, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **policy map** *name* | Configure a policy map.[1] |
| Step 2 | **class** *voice* | Specify the class for queuing. |
| Step 3 | **priority** *bandwidth* | Specify the bandwidth for this strict priority queue. |

[1] Total bandwidth for the policy map may not exceed 75 percent of the total PVC bandwidth.

## Associating the Policy Map to the ATM PVC

Follow the steps below to associate the policy map to the ATM PVC, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **interface ATM 0** | Enter configuration mode for the ATM interface. |
| Step 2 | **dsl equipment-type** {**co** \| **cpe**} | Configure the DSL equipment type. |
| Step 3 | **dsl linerate** {*number*\| **auto**} | Specify the ADSL line rate. The range of valid numbers is between 72 and 2312. |

| | Command | Task |
|---|---|---|
| Step 4 | **ip address** *ip-address mask* | Set the IP address and subnet mask for the ATM interface. |
| Step 5 | **pvc** *vpi/vci* | Create an ATM PVC for each end node with which the router communicates. |
| Step 6 | **encapsulation** *protocol* | Specify the encapsulation type for the PVC. Encapsulations can be specified as either AAL5SNAP or AAL5MUX PPP. |
| Step 7 | **service policy out** *name* | Associate the service policy name. |
| Step 8 | **vbr-rt** *pcr scr bs* | Specify the service class. |
| Step 9 | **exit** | Exit configuration mode for the ATM PVC. |

## Configuring Link Fragmentation and Interleaving with Low Latency Queuing

Link fragmentation and interleaving (LFI) is available when you are using multilink PPP over ATM.

Two types of traffic can be simultaneously transmitted over the same link:

- Large packets from heavy, delay-insensitive traffic sources
- Small packets from delay-sensitive traffic sources

The purpose of LFI is to reduce latency for delay-sensitive traffic. Two things happen when LFI is used:

- Large packets received from delay-insensitive sources are fragmented.
- Small packets received from delay-sensitive sources are interleaved with the large packet fragments.

Multilink PPP is one example of how LFI is implemented.

Use the following steps to configure the router for LFI. Begin in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **bandwidth** *bandwidth-kpts* | Configure the dialer bandwidth, The bandwidth configured under the dialer interface must be the same as the bandwidth allocated to its assigned PVC. |
| Step 2 | **ppp multilink** | Enable ppp multilink. |
| Step 3 | **ppp multilink interleave** | Specify ppp multilink interleaving. |
| Step 4 | **ppp multilink fragment-delay** *milliseconds* | Define the fragment delay. |
| Step 5 | **access-list** *access-list-number* {**permit** \| **deny**} *address mask* **precedence** *number* | Create an access list. |
| Step 6 | **class-map match-all voice** | Create a class map. |
| Step 7 | **match access-group** *number* | Link the class map to the access list. |
| Step 8 | **policy-map** *name* | Create a policy map. |
| Step 9 | **class** *name* | Define the class. |
| Step 10 | **priority** *number* | Assign priority bandwidth to the traffic. |
| Step 11 | **interface dialer** *number* | Define a dialer rotary group. |
| Step 12 | **service-policy** {**input** \| **output**} *policy-map* | Create a service policy. |

Calculate the fragment size using the following formula:

fragment size = (bandwidth in kbps/8) * fragment-delay i milliseconds (ms)

In this case, the fragment size = (640/8) * 10 = 800. The fragment size is greater than the maximum voice packet size of 200, which is that of G.711, 20 ms. Note that a low fragment delay corresponds to a fragment size that may be smaller than the voice packet size, resulting in reduced voice quality.

**Note** LFI should not be used when you have a link that exceeds 1 Mbps because, at this high speed, the latency of sending a big packet is small enough that the benefit of LFI is not required. Using LFI may actually increase latency because the extra processing time required to fragments packets may become a bottleneck.

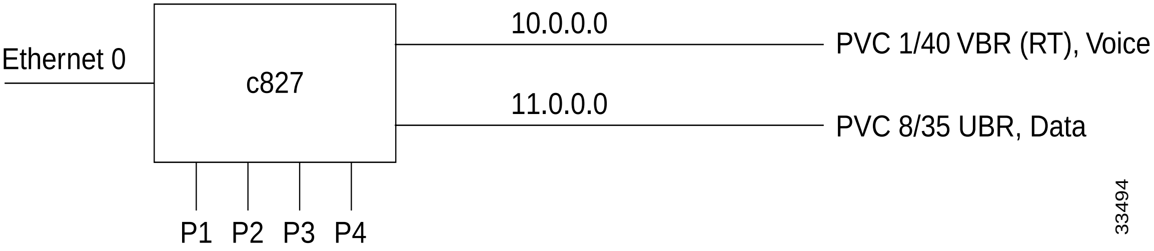
# Configuring a Multiple-PVC Environment

In a multiple-PVC environment, the traffic relies on the ATM interface to provide priority queuing for voice and fragmentation and interleaving. The following sections describe the configurations that you can use.

## Voice and Data on Different Subnets

Figure 7-2 shows voice and data packets on different subnets. All voice traffic may be on an ATM PVC with a vbr-rt service class, while all data traffic is transported on an ATM PVC with a ubr service class.

*Figure 7-2 Voice and Data on Different Subnets*



## Configuring the ATM Interface and Subinterfaces

Follow the steps below to configure the ATM interface and subinterfaces, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| **Step 1** | **interface ATM 0.1 point-to-point** | Specify the ATM0.1 subinterface. |
| **Step 2** | **ip address** *ip-address mask* | Set the IP address and subnet mask for the ATM0.1 subinterface. |
| **Step 3** | **pvc** *vpi/vci* | Create an ATM PVC for each end node with which the router communicates. |

| | Command | Task |
|---|---|---|
| Step 4 | **encapsulation** *type* | Specify the encapsulation type for the PVC. |
| Step 5 | **protocol ip** *address* **broadcast** | Set the protocol broadcast for the IP address. |
| Step 6 | **interface ATM 0.2 point-to-point** | Specify the ATM0.2 subinterface. |
| Step 7 | **ip address** *ip-address mask* | Set the IP address and subnet mask for the ATM0.2 subinterface. |
| Step 8 | **pvc** *vpi/vci* | Create an ATM PVC for each end node with which the router communicates. |
| Step 9 | **encapsulation** *type* | Specify the encapsulation type for the PVC. |
| Step 10 | **protocol ip** *address* **broadcast** | Set the protocol broadcast for the IP address. |
| Step 11 | **exit** | Exit configuration mode for the ATM interface. |

## Configuration Example

The following example shows a voice QoS configuration with all data traffic on the 30.0.0.1 network and all voice traffic on the 20.0.0.1 network.

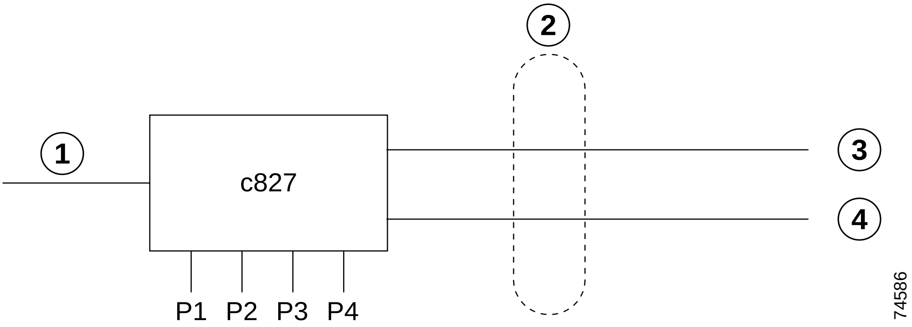
You do not need to enter the commands marked “default.” These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

```
!
interface ATM0.1 point-to-point
ip address 20.0.0.1 255.0.0.0
no ip directed-broadcast (default)
    pvc 1/100
protocol ip 20.0.0.2 broadcast
    vbr-rt 424 424 5
    encapsulation aal5snap
!
interface ATM0.2 point-to-point
ip address 30.0.0.1 255.0.0.0
no ip directed-broadcast (default)
pvc 1/101
protocol ip 30.0.0.2 broadcast
encapsulation aal5snap
```

# Voice and Data on the Same Subnet Using Virtual Circuit Bundling

Figure 7-3 and Table 7-2 show voice and data packets on the same subnet using virtual circuit bundling. Virtual circuit bundling allows multiple PVCs on the same bundle. Using virtual circuit bundling and assigning precedence 5 to voice packets and not data packets ensures that traffic for the two are separated onto two PVCs.

*Figure 7-3 Voice and Data on the Same Subnet with Virtual Circuit Bundling*



| Callout Number | Description |
|---|---|
| **1** | Ethernet 0 |
| **2** | Bundle |
| **3** | PVC Bundle 1/40 BVR (RT), voice |
| **4** | PVC Bundle 8/35 UBR, data |

The tasks for configuring a voice and data network on the same subnet with virtual circuit bundling are as follows:

- Configuring the ATM interface
- Configuring the PVC-bundle for voice
- Configuring the PVC-bundle for data
- Configuring IP Precedence for voice packets

## Configuring the ATM Interface, PVC-Bundle for Voice and Data, and IP Precedence for Voice Packets

Follow the steps below to configure the ATM interface, the PVC-bundle for voice and data, and IP Precedence for the voice packets, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **interface ATM 0** | Enter configuration mode for the ATM interface. |
| Step 2 | **dsl equipment-type** *co/cpe* | Configure the DSL equipment type. |
| Step 3 | **dsl linerate** *number/auto* | Specify the G.SHDSL line rate. The range of valid numbers is between 72 and 2312. |
| Step 4 | **dsl operating-mode gshdsl symmetric annex** *annex* | Set the G.SHDSL operating mode, and select the G.991.2 annex. |
| Step 5 | **ip address** *ip-address mask* | Set the IP address and subnet mask for the ATM interface. |
| Step 6 | **bundle** *name* | Specify a bundle name. |
| Step 7 | **encapsulation** *type* | Specify the encapsulation type for the voice bundle PVC. |
| Step 8 | **protocol ip** *ip-address* **broadcast** | Set the protocol broadcast for the IP address. |
| Step 9 | **pvc-bundle** *name vpi/vci* | Create a PVC for the voice bundle. |
| Step 10 | **vbr-rt** *pcr scr bs* | Set the service class for the voice bundle.[1] |
| Step 11 | **ip precedence** *number* | Select an IP Precedence level specific to the voice bundle that you created. |

| | Command | Task |
|---|---|---|
| Step 12 | **pvc-bundle** *name vpi/vci* | Create a PVC for the data bundle. |
| Step 13 | **ubr** *pcr* | Set the service class for the data[2] bundle. |
| Step 14 | **precedence** *other* | Set the IP Precedence level *other* to the data bundle that you created. |
| Step 15 | **exit** | Exit configuration mode for the ATM interface. |

1. For voice, the service class must be vbr-rt or vbr-nrt.
2. For data, the service class must be vbr-nrt or ubr.

# Specifying IP Precedence and the Service Class for the Voice Network

Follow the steps below to configure real-time voice traffic precedence over other IP network traffic, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **dial-peer voice** *number* **voip** | Enter the dial peer configuration mode to configure a VoIP dial peer. |
| Step 2 | **destination-pattern** *number* | Set a destination pattern. |
| Step 3 | **session target** {**ipv4**:*destination-address*} | Specify a destination IP address for the dial peer. |
| Step 4 | **precedence** *number* | Select a precedence level for the voice traffic associated with that dial peer. |

**Note** In IP Precedence, the numbers 1 through 5 identify classes for IP flows; the numbers 6 through 7 are used for network and backbone routing and updates. It is recommended that IP Precedence 5 is used for voice packets.

## Configuration Example

The following configuration shows both voice and data on the same subnet with virtual circuit bundling. IP precedence is set to 5 for the voice packets, but not for the data packets so that the traffic can be separated onto two different ATM PVCs.

```
!
interface atm0
ip address 20.0.0.1 255.0.0.0
bundle test
    encapsulation aal5snap
    protocol ip 20.0.0.2 broadcast
!
pvc-bundle voice 1/100
vbr-rt 424 424 5
precedence 5
!
pvc-bundle data 1/101
precedence other
!

dial-peer voice 100 voip
destination-pattern 26..
session target ipv4:20.0.0.8
ip precedence 5
!
```

# Configuring Dial Backup

You must decide whether to activate the backup interface when the primary line goes down, when the traffic load on the primary line exceeds the defined threshold, or when either occurs. The tasks you perform depend on your decision. Perform the tasks in the following sections to configure dial backup:

- Specifying the Backup Interface (mandatory)
- Defining Backup Line Delays (optional)
- Defining Traffic Load Threshold (optional)

Then configure the backup interface for DDR, so that calls are placed as needed.

## Specifying the Backup Interface

To specify a backup interface for a primary WAN interface or subinterface, enter the **backup interface** *type number* command to select a backup interface.

**Note** When you use a BRI for a dial backup, neither of the B channels can be used while the interface is in standby mode. In addition, when a BRI is used as a backup interface and the BRI is configured for legacy DDR, only one B channel is usable. Once the backup is initiated over one B channel, the second B channel is unavailable. When the backup interface is configured for dialer profiles, both B channels can be used.

For more information regarding the available dial backup mechanisms in IOS, please go to the following URL:

http://www.cisco.com/warp/public/123/backup-main.html

## Defining Backup Line Delays

You can configure a value that defines how much time should elapse before a secondary line status changes after a primary line status has changed. You can define two delays:

- A delay that applies after the primary line goes *down* but before the secondary line is activated
- A delay that applies after the primary line comes *up* but before the secondary line is deactivated

To define these delays, use the following syntax:

Router (config-if) # **backup delay** {enable-delay | **never**} {disable-delay | **never**}

# Defining Traffic Load Threshold

You can configure dial backup to activate the secondary line, based on the traffic load on the primary line. The software monitors the traffic load and computes a 5-minute moving average. If this average exceeds the value you set for the line, the secondary line is activated and, depending on how the line is configured, some or all of the traffic will flow onto the secondary dialup line.

You can configure a load level for traffic at which additional connections will be added to the primary WAN interface. The load level values range from 1 (unloaded) to 255 (fully loaded).

Use the following syntax to define a WAN line threshold:

Router (config-if) # **dialer load-threshold 8 outbound** {enable-threshold | **never**} {disable-threshold | **never**}

# Dial Backup Using the Console Port

The following example shows dial backup using a console port configured for DDR:

```
interface atm 0
 ip address 172.30.3.4 255.255.255.0
 backup interface async1
 backup delay 10 10
 !
interface async 1
 ip address 172.30.3.5 255.255.255.0
 dialer in-band
 dialer string 5551212
 dialer-group 1
 async dynamic routing
 dialer list 1 protocol ip permit
chat-script sillyman “““atdt 5551212” TIMEOUT 60 “CONNECT”
line aux 0
 modem chat-script sillyman
 modem inout
speed 9600
```

# Configuration Example

The following example shows configuration of dial backup and remote router management on the Cisco 831 and Cisco 837 routers using the console port and dialer watch.

```
!
username Router password !PASSWORD
!
modemcap entry MY_USR_MODEM:MSC=&F1S0=1
!
chat-script Dialout ABORT ERROR ABORT BUSY "" "AT" OK "ATDT 5555102\T"
TIMEOUT 60 CONNECT \c
!
interface Async1
 no ip address
 encapsulation ppp
 dialer in-band
 dialer pool-member 3
 autodetect encapsulation ppp
 async default routing
 async dynamic routing
 async mode dedicated
 pap authentication pap callin
!
! Dialer3 is for dial backup and remote router management
!
interface Dialer3
 ip address negotiated
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 dialer pool 3
 dialer remote-name !REMOTE-NAME
 dialer idle-timeout 300
 dialer string 5555102 modem-script Dialout
 dialer watch-group 1
 dialer-group 1
 autodetect encapsulation ppp
 peer default ip address 192.168.2.2
 no cdp enable
 ppp pap sent-username ! USER SPECIFIC password ! USER SPECIFIC
 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
ip route 0.0.0.0 0.0.0.0 !(dial backup peer address @ISP)
ip route 0.0.0.0 0.0.0.0 Dialer1 150
!
no ip http server
ip pim bidir-enable
!
!
access-list 101 permit ip 192.168.0.0 0.0.255.255 any
dialer watch-list 1 ip !(ATM peer address @ISP) 255.255.255.255
dialer-list 1 protocol ip permit
!
! To direct traffic to an interface only if the Dialer gets assigned
with an ip address
 route-map main permit 10
  match ip address 101
  match interface Dialer1
 !
 route-map secondary permit 10
  match ip address 101
  match interface Dialer3
!
line con 0
 exec-timeout 0 0
 modem enable
 stopbits 1
line aux 0
 exec-timeout 0 0
 script dialer Dialout
 modem InOut
 modem autoconfigure type MY_USR_MODEM
 transport input all
 stopbits 1
 speed 38400
 flowcontrol hardware
line vty 0 4
 exec-timeout 0 0
 login local
!
```

The following example shows configuration of remote management using a console port for the Cisco SOHO 91 and Cisco SOHO 97 routers.

```
!
username Router password !PASSWORD
!
```

```
modemcap entry MY_USR_MODEM:MSC=&F1S0=1
!
interface Async1
 no ip address
 encapsulation ppp
 dialer in-band
 autodetect encapsulation ppp
 async default routing
 async dynamic routing
 async mode dedicated
 pap authentication pap callin
 peer default ip address pool clientpool
 !
! dialer 1 used for PPPoE or PPPoATM
! PPPoE or PPPoATM dialer1 configurations are not shown in this sample
!
ip route 0.0.0.0 0.0.0.0 dialer 1 150
!
dialer list 1 protocol ip permit
!
ip local pool clientpool 192.168.0.2 192.168.0.10
!
line con 0
 exec-timeout 0 0
 modem enable
 stopbits 1
line aux 0
 exec-timeout 0 0
 modem Dialin
 modem autoconfigure type MY_USER_MODEM
 transport input all
 stopbits 1
 speed 38400
 flowcontrol hardware
 to align with line aux 0
 exec-timeout 0 0
 login local
!
```

# Configuration Example

The following example shows dial backup and remote management configuration on the Cisco 836 router, using the ISDN S/T port and dialer watch.

```
Cisco836#
!
```

```
vpdn enable
!
vpdn-group 1
 accept-dialin
 protocol pppoe
!
!Specifies the ISDN switch type
isdn switch-type basic-net3
!
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
 hold-queue 100 out
!
!ISDN interface to be used as a backup interface
interface BRI0
 no ip address
 encapsulation ppp
 dialer pool-member 1
 isdn switch-type basic-net3
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 pvc 1/40
   encapsulation aal5snap
   pppoe-client dial-pool-number 2
 !
 dsl operating-mode auto
!
! Dial backup interface, associated with physical BRI0 interface.
Dialer pool 1 associates it with BRI0’s dialer pool member 1. Note
“dialer watch-group 1” associates a watch list with corresponding
“dialer watch-list” command
interface Dialer0
 ip address negotiated
 encapsulation ppp
 dialer pool 1
 dialer idle-timeout 30
 dialer string 384040
 dialer watch-group 1
 dialer-group 1
!
! Primary interface associated with physical ATM0 interface, dialer
pool 2 associates it with ATM0’s dial-pool-number2
interface Dialer2
 ip address negotiated
 ip mtu 1492
 encapsulation ppp
 dialer pool 2
 dialer-group 2
 no cdp enable
!
ip classless

!Primary and backup interface given route metric
ip route 0.0.0.0 0.0.0.0 22.0.0.2
ip route 0.0.0.0 0.0.0.0 192.168.2.2 80
ip http server
!
!Watch for interesting traffic
dialer watch-list 1 ip 22.0.0.2 255.255.255.255

!Specifies interesting traffic to trigger backup ISDN traffic
dialer-list 1 protocol ip permit
!
```

# Configuring IGMP Proxy and Sparse Mode

The Internet Group Management Protocol (IGMP) proxy feature was added to the unidirectional link routing feature to permit hosts that are not directly connected to a downstream router to join a multicast group sourced from an upstream network.

Follow the steps below to configure IGMP proxy and sparse mode, starting in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **ip multicast-routing** | Enable IP multicast forwarding. |
| Step 2 | **ip pim rp-address** *address* | Configure the Protocol Independent Multicast (PIM) Rendezvous Point (RP) address. |
| Step 3 | **interface ethernet 0** | Enter Ethernet 0 interface configuration mode. |
| Step 4 | **ip address** *ip-address subnet-mask* | Configure an IP address and subnet mask for the Ethernet 0 interface. |
| Step 5 | **ip pim** { **sparse** \|**dense** }**-mode** | Configure the Ethernet 0 interface for PIM sparse mode or PIM dense mode. |
| Step 6 | **interface Ethernet 1** | Enter Ethernet 1 configuration mode. |

| | Command | Task |
|---|---|---|
| Step 7 | **ip address** {*ip-address subnet-mask* ***negotiated***} | Specify an IP address and subnet mask for the dialer interface, or indicate that the IP address is to be negotiated. |
| Step 8 | **ip pim** {*sparse* \| *dense*} **-mode** | Configure the dialer interface for PIM sparse mode or PIM dense mode. |
| Step 9 | **ip igmp mroute-proxy loopback 0** | When used with the **ip igmp proxy-service** command, this command enables all forwarding entries in the multicast forward table of IGMP to report to a proxy service interface. |
| Step 10 | **end** | Exit router configuration mode. |
| Step 11 | **interface loopback 0** | Enter loopback interface configuration mode. |
| Step 12 | **ip address** *ip-address subnet-mask* | Configure an IP address and subnet mask for the loopback 0 interface. |
| Step 13 | **ip pim sparse-mode** | Configure the loopback interface for PIM sparse mode or PIM dense mode. |
| Step 14 | **ip igmp helper-address udl ethernet 0** | Enter IGMP helper-address unidirectional link to Ethernet 0 |
| Step 15 | **ip igmp proxy-service** | Enable the multicast route proxy service. Based on the IGMP query interval, the router periodically checks the mroute table for forwarding entries that match interfaces configured with the **ip igmp mroute-proxy** command. Where there is a match, one IGMP report is created and received on this interface. This command is intended to be used with the **ip igmp helper-address udl** command, which forwards the IGMP report to an upstream router. |

# Configuration Example

The following example shows the relevant IGMP proxy and sparse mode commands. The Ethernet 0, Ethernet 1, and loopback 0 interfaces have been configured for PIM sparse mode; the PIM RP address has been defined as 10.5.1.1.

```
ip pim rp-address 10.5.1.1 5
access-list 5 permit 239.0.0.0 255.255.255.255
!
interface loopback 0
ip address 10.7.1.1 255.255.255.0
ip pim sparse-mode
ip igmp helper-address udl ethernet 0
ip igmp proxy-service
!
interface ethernet 0
ip address 10.2.1.2 255.255.255.0
ip pim sparse-mode
ip igmp unidirectional link
!
interface ethernet 1
ip address 10.5.1.1 255.255.255.0
ip pim sparse-mode
ip igmp mroute-proxy loopback 0
!
```

## Verifying Your Configuration

You can verify your configuration by using the **show ip igmp interface ethernet 0** multicasting command. You should see a verification output similar to the following:

```
router#show ip igmp interface ethernet 0
Ethernet0 is up, line protocol is up
    Internet address is 10.2.1.2 255.255.255.0
    IGMP is enabled on interface
    Current IGMP host version is 2
    Current IGMP router version is 2
    IGMP query interval is 60 seconds
    IGMP querier timeout is 120 seconds
    IGMP max query response time is 10 seconds
    Last member query response interval is 1000 ms
    Inbound IGMP access group is not set
    IGMP activity: 1 joins, 0 leaves
    Multicast routing is enabled on interface
    Multicast designated router (DR) is 10.2.1.2 (this system)
    IGMP querying router is 10.2.1.2 (this system)
    Multicast groups joined (number of users):
        224.0.1.40 (1)
```

# Configuring IP Security and GRE Tunneling

IP Security (IPSec) provides secure tunnels between two peers, such as two routers. You can define which packets are to be considered sensitive and sent through these secure tunnels. You can also define the parameters which should be used to protect these sensitive packets, by specifying characteristics of these tunnels. When the IPSec peer sees a sensitive packet, it sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer.

This section contains the following topics:

- Configuring Internet Protocol Parameters
- Configuring an Access List
- Configuring IPSec
- Configuring a GRE Tunnel Interface
- Configuring the Ethernet Interface
- Configuring Static Routes
- Configuring and Monitoring High-Speed Crypto
- Configuration Example

Configurations for both IPSec and Generic Routing Encapsulation (GRE) tunneling are presented in this section. Perform the following steps to configure IPSec using a GRE tunnel, beginning in global configuration mode.

For general IPSec configuration, go to:

www.cisco.com/warp/public/707/index.shtml#ipsec

## Configuring Internet Protocol Parameters

Complete the follow steps to configure IP parameters, starting in global configuration mode.

| | Command | Task |
|---|---|---|
| **Step 1** | **ip subnet-zero** | Configure the router to recognize the zero subnet range as the valid range of addresses. |
| **Step 2** | **no ip finger** | Block incoming IP finger packets. |
| **Step 3** | **no ip domain-lookup** | Disable the router from interpreting unfamiliar words (typographical errors) as host names entered during a console session. |
| **Step 4** | **ip classless** | Follow classless routing forwarding rules. |

## Configuring an Access List

Use the **access-list** command to create an access list that permits the GRE protocol and that specifies the starting and ending IP addresses of the GRE tunnel. Use the following syntax:

**access-list 101 permit gre host** *ip-address* **host** *ip-address*

In the preceding command line, the first **host** *ip-address* specifies the tunnel starting point, and the second **host** *ip-address* specifies the tunnel end point.

## Configuring IPSec

Follow the steps below to configure IPSec, starting in global configuration mode.

| | Command | Task |
|---|---|---|
| **Step 1** | **crypto isakmp policy 10** | Define an Internet Key Exchange (IKE) policy, and assign the policy a priority. This command places the router in IKE policy configuration mode. |
| **Step 2** | **hash md5** | Specify the md5 hash algorithm for the policy. |
| **Step 3** | **authentication pre-share** | Specify pre-share key as the authentication method. |
| **Step 4** | **exit** | Exit IKE policy configuration mode. |

| | Command | Task |
|---|---|---|
| Step 5 | **crypto isakmp key** *name* **address** *ip-address* | Configure a pre-shared key and static IP address for each VPN client. |
| Step 6 | **crypto ipsec transform-set** *name* **esp-des esp-md5-hmac** | Define a combination of security associations to occur during IPSec negotiations. |
| Step 7 | **crypto map** *name* **local-address ethernet 1** | Create a crypto map, and specify and name an identifying interface to be used by the crypto map for IPSec traffic. |
| Step 8 | **crypto map** *name seq-num* **ipsec-isakmp** | Enter crypto map configuration mode, and create a crypto map entry in IPSec ISAKMP mode. |
| Step 9 | **set peer** *ip-address* | Identify the remote IPSec peer. |
| Step 10 | **set transform-set** *name* | Specify the transform set to be used. |
| Step 11 | **match address** *access-list-id* | Specify an extended access list for the crypto map entry. |
| Step 12 | **exit** | Exit crypto map configuration mode. |

## Configuring a GRE Tunnel Interface

Follow the steps below to configure the generic routing encapsulation (GRE) tunnel interface, starting in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **interface tunnel 0** | Configure the tunnel 0 interface. |
| Step 2 | **ip address** *ip-address subnet-mask* | Set the IP address and subnet mask for the tunnel 0 interface. |
| Step 3 | **tunnel source ethernet 1** | Specify the Ethernet 1 interface as the tunnel source. |
| Step 4 | **tunnel destination** *default-gateway-ip-address* | Specify the default gateway as the tunnel destination. |

| | Command | Task |
|---|---|---|
| **Step 5** | **crypto map** *name* | Associate a configured crypto map to the tunnel 0 interface. |
| **Step 6** | **exit** | Exit the tunnel 0 interface configuration. |

## Configuring the Ethernet Interfaces

Perform the following tasks to configure the Ethernet 0 and Ethernet 1 interfaces, starting in global configuration mode.

| | Command | Task |
|---|---|---|
| **Step 1** | **interface ethernet 0** | Configure the Ethernet 0 interface. |
| **Step 2** | **ip address** *ip-address subnet-mask* | Set the IP address and subnet mask for the Ethernet 0 interface. |
| **Step 3** | **exit** | Exit the Ethernet 0 interface configuration. |
| **Step 4** | **interface ethernet 1** | Configure the Ethernet 1 interface. |
| **Step 5** | **ip address** *ip-address subnet-mask* | Set the IP address and subnet mask for the Ethernet 1 interface. |
| **Step 6** | **crypto map** *name* | Associate a crypto map with the Ethernet 1 interface. |
| **Step 7** | **end** | Exit router configuration mode. |

## Configuring Static Routes

Complete the following steps to configure static routes, starting in global configuration mode.

| | Command | Task |
|---|---|---|
| **Step 1** | **ip route** *default-gateway-ip-address mask* **ethernet 1** | Create a static route for the Ethernet 1 interface. |
| **Step 2** | **ip route** *default-gateway-ip-address mask* **tunnel 0** | Create a static route for the tunnel 0 interface. |
| **Step 3** | **ip route** *default-gateway-ip-address mask gateway-of-last-resort* | Create a static route to the gateway of last resort. |
| **Step 4** | **end** | Exit router configuration mode. |

## Configuring and Monitoring High-Speed Crypto

Use the following command to enable high-speed crypto, starting with global configuration mode.

```
crypto engine accelerator
```

To disable high-speed crypto, use the following command:

```
no crypto engine accelerator
```

To monitor high-speed crypto, use the following command:

```
show crypto engine accelerator statistic
```

For more information on configuring IPSec, refer to the *Cisco IOS Security Configuration Guide*.

## Configuration Example

This configuration example for the Cisco 831 router shows IPSec being used over a GRE tunnel. The example also applies to a Cisco SOHO 91 router. You do not need to enter the commands marked “default.” These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

```
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 831-uut1
!
memory-size iomem 10
!
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
crypto isakmp key grel address 100.1.1.1
!
crypto ipsec security-association lifetime seconds 86400
!
crypto ipsec transform-set strong esp-3des esp-sha-hmac
!
crypto map mymap local-address Ethernet1
crypto may mymap 1 ipsec-isakmp
 set peer 100.1.1.1
 set transform-set strong
 match address 151
!
!
!
!
interface Tunnel0
 ip address 1.1.1.1 255.255.255.0
 tunnel source Ethernet1
 tunnel destination 100.1.1.1
 crypto map mymap
!
interface Ethernet0
 ip address 202.2.2.2 255.255.255.0
 hold-queue 100 out
!
interface Ethernet1
 ip address 100.1.1.1 255.255.255.0
 crypto map mymap
!
ip classless
ip route 200.1.1.0 255.255.255.0 Tunnel0
ip http server
!
```

```
!
access-list 151 permit gre host 100.1.1.2 host 100.1.1.1
!
line con 0
 no modem enable
 stopbits 1
line aux 0
line vty 0 4
!
scheduler max-task-time 5000
```

The following example shows IPSec configuration on a Cisco 837 router.

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 837-uutl
!
memory-size iomem 10
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
crypto isakmp key grel address 100.1.1.1
!
crypto ipsec transform-set strong esp-3des esp-sha-hmac
!
crypto map mymap local-address ATM0
crypto map mymap 1 ipsec-isakmp
 set peer 100.1.1.1
 set transform-set strong
 match address 151
!
interface Tunnel0
```

```
 ip address 1.1.1.1 255.255.255.0
 ip mtu 1440
 tunnel source ATM0
 tunnel destination 100.1.1.1
 crypto map mymap
!
interface Ethernet0
 ip address 202.2.2.2 255.255.255.0
 hold-queue 100 out
!
interface ATM0
 ip address 100.1.1.2 255.255.255.0
 no atm ilmi-keepalive
 pvc 1/40
  protocol ip 100.1.1.1 broadcast
  encapsulation aa15snap
 !
 dsl operating-mode auto
 crypto map mymap
!
ip classless
ip route 200.1.1.0 255.255.255.0 Tunnel0
ip http server
ip pim bidir-enable
```

# Configuring Multilink PPP Fragmentation and Interleaving

You should configure multilink PPP fragmentation if you have point-to-point connection using PPP encapsulation or if you have links slower than your network.

PPP support for interleaving can be configured on a dialer interface.

Follow the steps below to configure multilink PPP and interleaving on a dialer interface, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **interface dialer** | Enter configuration mode for the dialer interface. |
| Step 2 | **ppp multilink** | Enable multilink PPP for the dialer interface. |

| | Command | Task |
|---|---|---|
| Step 3 | **bandwidth** *n* | Specify the bandwidth number associated with the PVC that is using the dialer interface, where *n* is the value of the sustained cell rate (SCR) parameter of the PVC using that dialer interface.This is important because otherwise the dialer interface will assume a value of 100 kbps if a specific class of service is configured. |
| Step 4 | **ppp multilink interleave** | Enable interleaving for RTP packets among the fragments of larger packets on a multilink PPP bundle. |
| Step 5 | **ppp multilink fragment-delay** *milliseconds* | Configure a maximum fragment delay of 20 ms. This command is optional. |
| Step 6 | **ip rtp reserve** *lowest-UDP-port range-of-ports* [*maximum-bandwidth*] | Reserve a special queue for real-time packet flows to specified destination UDP ports, allowing real-time traffic to have higher priority than other flows. |
| Step 7 | **exit** | Exit configuration mode for the dialer interface. |

For complete information on the PPP fragmentation and interleaving commands, refer to the *Dial Solutions Configuration Guide* for Cisco IOS Release 12.0T. For general information on PPP fragmentation and interleaving concepts, see Chapter 1, “Concepts.”

## Configuration Example

The following configuration defines a dialer interface that enables multilink PPP with interleaving and a maximum real-time traffic delay of 20 ms. The encapsulation type is defined as *aal5mux*.

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

```
!
interface dialer 1
ppp multilink
encapsulated ppp
ppp multilink interleave
bandwidth 640
ppp multilink fragment-delay 20
ip rtp reserve 16384 100 64
!
interface ATM0
    pvc 8/35
    encapsulation aal5mux ppp dialer
dialer pool-member 1
```

## Verifying Your Configuration

To verify that you have properly configured PPP fragmentation and interleaving, enter the **debug ppp multilink fragment** command, and then send out one 1500-byte ping packet. The debug message will display information about the fragments being transmitted.

# Configuring IP Precedence

IP Precedence gives voice packets higher priority than other IP data traffic. Complete the following steps to configure real-time voice traffic precedence over other IP network traffic, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **configure terminal** | Enter configuration mode. |
| Step 2 | **dial-peer voice** *number* **voip** | Enter the dial peer configuration mode to configure a VoIP dial peer. |
| Step 3 | **destination-pattern** *number* | Set a destination pattern. |
| Step 4 | **ip precedence** *number* | Select a precedence level for the voice traffic associated with that dial peer. |

**Note** In IP Precedence, the numbers 1 through 5 identify classes for IP flows; the numbers 6 through 7 are used for network and backbone routing and updates.

For complete information on the IP Precedence commands, refer to the Cisco IOS Release 12.0 documentation set. For general information on IP precedence, see Chapter 1, "Concepts."

## Configuration Example

This configuration example shows a voice configuration with IP Precedence set. The IP destination target is set to 8 dialing digits, which automatically sets the IP precedence to 5 on the Cisco routers. The dial peer session target is RAS, which is a protocol that runs between the H.323 voice protocol gateway and gatekeeper.

You do not need to enter the commands marked "default." These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

```
!
access-list 101 permit
route-map data permit 10
set ip precedence routing
!
```

# Configuring Voice

| | Command | Task |
|---|---|---|
| **Step 1** | **configure dial-peer** | Enter configuration mode for the dial peer. |
| **Step 2** | **dial-peer voice** *number* **voip** | Assign the dial peer voice number to configure a VoIP dial peer. |

The Cisco 827 voice-enabled routers support voice using the H.323 signaling protocol as the default signaling protocol.

# Prerequisite Tasks

Before you can configure your router to use voice, you need to perform the following tasks:

- Establish a working IP network.
- Complete your company dial plan.
- Establish a working telephony network based on your company dial plan.
- Integrate your dial plan and telephony network into your existing IP network topology.

# Configuring Voice for H.323 Signaling

This section describes the tasks you need to perform to configure the router for H.323 signaling on the voice ports.

## Configuring the POTS Dial Peers

Use the following steps to configure the POTS dial peers, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| **Step 1** | **dial-peer voice** *number* **POTS** | Enter configuration mode for the dial peer. |
| **Step 2** | **destination-pattern** *string* | Define the destination telephone number associated with the VoIP dial peer. |
| **Step 3** | **port** *number* | Specify the port number. |

## Configuring Voice Dial Peers for H.323 Signaling

Complete the following steps to configure voice dial peers for H.323 signaling, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **dial-peer voice** *number* **VoIP** | Enter configuration mode for the dial peer. |
| Step 2 | **destination-pattern** *string* | Define the destination telephone number associated with each VoIP dial peer. |
| Step 3 | **codec** *string* | Specify a codec if you are not using the default codec of g.729. |
| Step 4 | **session target** {**ipv4**:*destination-address*} | Specify a destination IP address for each dial peer. |

## Configuring Voice Ports for H.323 Signaling

Voice port configuration should be automatic in the United States; however, for configuration outside the United States, you may follow the steps below to configure the voice port, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **configure dial-peer** | Enter configuration mode for the dial peer. |
| Step 2 | **voice-port** *port* | Identify the voice port you want to configure and enter the voice port configuration mode. |
| Step 3 | **cptone** *country* | Select the appropriate voice call progress tone for this interface. The default country for this command is **us**. |
| Step 4 | **ring frequency (25 \ 50)** | Select the ring frequency (in Hz) specific to the equipment attached to this voice port and appropriate to the country you are in. |
| Step 5 | **description** *string* | Attach descriptive text about this voice port connection. |
| Step 6 | **comfort-noise** | If voice activity detection (VAD) is activated, specify that background noise is generated. |
| Step 7 | **impedance** | Specify impedance, which is related to the electrical characteristics of the device that is plugged into a POTS port. Impedance is measured in ohms. |

For complete information on the dial peer commands, refer to the Cisco IOS Release 12.0 documentation set. For general information on dial peer concepts, see Chapter 1, "Concepts."

## Configuring Number Expansion

This section describes how to expand an extension number into a particular destination pattern. Use the following global configuration command to expand the extension number:

```
Router(config)# num-exp extension-number extension-string
```

To verify that you have mapped the telephone numbers correctly, enter the **show num-exp** command.

After you have configured dial peers and assigned destination patterns to them, enter the **show dialplan number** command to see how a telephone number maps to a dial peer.

For complete information on the number expansion commands, refer to the Cisco IOS documentation set.

## Configuration Example

This configuration shows voice traffic configured. You do not need to enter the commands marked "default." These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

```
!
class-map voice
match access-group 101
!
policy-map mypolicy
class voice
priority 128
class class-default
fair-queue 16
!
ip subnet-zero
!
gateway
!
interface Ethernet0
```

```
ip address 20.20.20.20 255.255.255.0
no ip directed-broadcast (default)
ip route-cache policy
ip policy route-map data
!
interface ATM0
ip address 10.10.10.20 255.255.255.0
no ip directed-broadcast (default)
no atm ilmi-keepalive (default)
pvc 1/40
service-policy output mypolicy
protocol ip 10.10.10.36 broadcast
vbr-nrt 640 600 4
! 640 is the maximum upstream rate of ADSL
encapsulation aal5snap
!
bundle-enable
h323-gateway voip interface
h323-gateway voip id gk-twister ipaddr 172.17.1.1 1719
h323-gateway voip h323-id gw-820
h323-gateway voip tech-prefix 1#
!
router eigrp 100
network 10.0.0.0
network 20.0.0.0
!
ip classless (default)
no ip http server
!
access-list 101 permit ip any any precedence critical
route-map data permit 10
set ip precedence routine
!
!
line con 0
exec-timeout 0 0
transport input none
stopbits 1
line vty 0 4
login
!
!
voice-port 1
local-alerting
timeouts call-disconnect 0
!
voice-port 2
local-alerting
```

```
timeouts call-disconnect 0
!
voice-port 3
local-alerting
timeouts call-disconnect 0
!
voice-port 4
local-alerting
timeouts call-disconnect 0
!
dial-peer voice 10 voip
destination-pattern........
ip precedence 5
session target ras
!
dial-peer voice 1 pots
destination-pattern 5258111
port 1
!
dial-peer voice 2 pots
destination-pattern 5258222
port 2
!
dial-peer voice 3 pots
destination-pattern 5258333
port 3
!
dial-peer voice 4 pots
destination-pattern 5258444
port 4
!
end
```

# Cisco 827 Router Configuration Examples

Examples are provided for the following configurations:

- Cisco 827-4V Router Configuration
- Cisco 827 Router Configuration
- Corporate or Endpoint Router Configuration for Data Network
- Corporate or Endpoint Router Configuration for Data and Voice Network

These configurations are intended to be examples only. Your router configuration may look different, depending on your network.

## Cisco 827-4V Router Configuration

The following is a configuration for the Cisco 827-4V router configured for H.323 signaling voice traffic. These commands appear automatically in the configuration file generated when you use the **show running-config** command.

```
ip subnet-zero
!
bridge crb
!
interface Ethernet0
no ip address
no ip directed-broadcast
bridge-group 1
!
interface ATM0
no ip address
no ip directed-broadcast
no atm ilmi-keepalive
bundle-enable
!
interface ATM0.1 point-to-point
ip address 1.0.0.1 255.255.255.0
no ip directed-broadcast
pvc voice 1/40
protocol ip 1.0.0.2 broadcast
encapsulation aal5snap
!
!
interface ATM0.2 point-to-point
no ip address
no ip directed-broadcast
pvc data 1/41
encapsulation aal5snap
!
bridge-group 1
!
ip classless
!
bridge 1 protocol ieee
!
voice-port 1
local-alerting
```

```
timeouts call-disconnect 0
!
voice-port 2
local-alerting
timeouts call-disconnect 0
!
voice-port 3
local-alerting
timeouts call-disconnect 0
!
voice-port 4
local-alerting
timeouts call-disconnect 0
!
dial-peer voice 101 pots
destination-pattern 14085271111
port 1
!
dial-peer voice 1100 voip
destination-pattern 12123451111
codec g711ulaw
session target ipv4:1.0.0.2
!
dial-peer voice 102 pots
destination-pattern 14085272222
port 2
!
dial-peer voice 1200 voip
destination-pattern 12123452222
codec g711ulaw
session target ipv4:1.0.0.2
!
dial-peer voice 103 pots
destination-pattern 14085273333
port 3
!
dial-peer voice 1300 voip
destination-pattern 12123453333
codec g711ulaw
session target ipv4:1.0.0.2
!
dial-peer voice 104 pots
destination-pattern 14085274444
port 4
!
dial-peer voice 1400 voip
destination-pattern 12123454444
codec g711ulaw
```

```
session target ipv4:1.0.0.2
!
```

## Cisco 827 Router Configuration

The following is a configuration for the Cisco 827 router. You do not need to enter the commands marked “default.” These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

```
Current configuration:
!
version 12.0
no service pad (default)
service timestamps debug uptime (default)
service timestamps log uptime (default)
no service password-encryption (default)
hostname Cisco827
enable secret 5 $1$RnI.$K4mh5q4MFetaqKzBbQ7gv0
ip subnet-zero
no ip domain-lookup
ip dhcp-server 20.1.1.2
ipx routing 0010.7b7e.5499
!In the preceding command, the router MAC address is automatically
used ! as the router IPX address.
!
interface Ethernet0
ip address 10.1.1.1 255.255.255.0
no ip directed-broadcast (default)
ipx network 100 novell-ether
!
interface ATM0
 ip address 14.0.0.17 255.0.0.0
 no ip directed-broadcast (default)
 no atm ilmi-keepalive (default)
pvc 8/35
  protocol ip 14.0.0.1 no broadcast
  encapsulation aal5snap
!
router rip
version 2
network 10.0.0.0
network 30.0.0.0
no auto-summary
!
no ip http server (default)
```

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

# Corporate or Endpoint Router Configuration for Data Network

This section shows a configuration that you can use to configure a Cisco 3600 router as a corporate or endpoint router in your data network.You do not need to enter the commands marked “default.” These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

```
Current configuration:
!
version 12.0
no service pad (default)
service timestamps debug uptime (default)
service timestamps log uptime (default)
no service password-encryption (default)
!
hostname c3600
enable secret 5 $1$8TI8$WjLcYWgZ7EZhqH49Y2hJV!
ip subnet-zero
no domain-lookup
ipx routing 0010.7b7e.5498
!In the preceding command, the router MAC address is automatically
used as the router IPX address.
!
interface Ethernet0
 ip address 20.0.0.1 255.0.0.0
 no ip directed-broadcast (default)
ipx network 200
!
router rip
version 2
network 20.0.0.0
network 30.0.0.0
no auto-summary
!
no ip http server (default)
ip classless (default)
!
protocol ip 2.0.0.1 broadcast
!
line con 0
 exec-timeout 0 0
 transport input none (default)
 stopbits 1 (default)
line vty 0 4
password secret
login
!
end
```

# Corporate or Endpoint Router Configuration for Data and Voice Network

This section shows a configuration that you can use to configure a Cisco 3600 router as a corporate or endpoint router in your data and voice network.You do not need to enter the commands marked “default.” These commands appear automatically in the configuration file generated when you use the **show running-config** command.

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname c3640
!
ip subnet-zero
!
cns event-service server
!
!
!
voice-port 1/0/0
 no echo-cancel enable
```

```
!
voice-port 1/1/0
!
voice-port 1/1/1
!
dial-peer voice 101 pots
 destination-pattern 5552222
 port 1/0/0
!
dial-peer voice 102 pots
 destination-pattern 5554444
 port 1/0/1
!
dial-peer voice 103 pots
 destination-pattern 5556666
 port 1/1/0
!
dial-peer voice 104 pots
 destination-pattern 5558888
 port 1/1/1
dial-peer voice 1100 voip
 destination-pattern 5551111
 codec g711alaw
 ip precedence 5
 no vad
 session target ipv4:2.0.0.3
!
dial-peer voice 1101 voip
 destination-pattern 5553333
 codec g711alaw
 ip precedence 5
 no vad
 session target ipv4:2.0.0.3
!
dial-peer voice 1102 voip
 destination-pattern 5555555
 codec g711alaw
 ip precedence 5
 session target ipv4:2.0.0.3
!
dial-peer voice 1103 voip
 destination-pattern 5557777
 codec g711alaw
 ip precedence 5
 session target ipv4:2.0.0.3
!
process-max-time 200
!
```

```
interface Ethernet0/1
 no ip address
 no ip directed-broadcast (default)
shutdown
!
router rip
version 2
network 3.0.0.0
!
ip classless (default)
ip route 0.0.0.0 0.0.0.0 Ethernet 0/0
ip route 1.0.0.0 255.0.0.0 3.0.0.0
ip route 2.0.0.0 255.0.0.0 3.0.0.1

ip route 5.0.0.0 255.0.0.0 3.0.0.1
ip route 40.0.0.0 255.255.255.0 172.28.9.1
ip route 172.28.5.0 255.255.255.0 172.28.9.1
ip route 172.28.9.0 255.255.255.0 172.28.9.1
no http server
!
line con 0
transport input none (default)
line aux 0
line vty 0 4
login
!
end
```

CHAPTER 8

# Advanced Router Configuration

This chapter includes advanced configuration procedures for the Cisco 800 series and Cisco SOHO series routers.

**Note** Every feature described is not necessarily supported on every router model. Where possible and applicable, these feature limitations will be listed.

If you prefer to use network scenarios to build a network, see Chapter 4, "Network Scenarios." For basic router configuration topics, see Chapter 7, "Router Feature Configuration."

This chapter contains the following sections:

- Configuring IP Named Access Lists, page 8-29
- Configuring International Phone Support, page 8-29
- Configuring Committed Access Rate, page 8-36
- Configuring VPN IPSec Support Through NAT, page 8-37
- NAT Default Inside Server Enhancement, page 8-38
- Configuring VoAAL2 ATM Forum Profile 9 Support, page 8-40
- Configuring ATM OAM F5 Continuity Check Support, page 8-44
- Configuring RADIUS Support, page 8-49
- Configuring Cisco Easy VPN Client, page 8-49
- Configuring Dial-on-Demand Routing for PPPoE Client, page 8-52
- Configuring Weighted Fair Queuing, page 8-55
- Configuring DSL Commands, page 8-57
- Configuring FTP Client, page 8-63
- Configuring Authentication Proxy, page 8-63
- Configuring Port to Application Mapping, page 8-64
- Configuring CBAC Audit Trails and Alerts, page 8-64

Each section includes a configuration example and verification steps, as available.

In some instances, certain features are supported across all Cisco 800 series and Cisco SOHO series router models. Router model feature restrictions or requirements are also listed in each applicable section in this chapter.

# Configuring Support for PPP over Ethernet

The following sections describe how to configure support for PPP over Ethernet (PPPoE).

- Configuring PPPoE Client Support
- Configuring TCP Maximum Segment Size for PPPoE

# Configuring PPPoE Client Support

PPPoE is supported on the following Cisco routers:

- Cisco 806 and 831
- Cisco 826 and 836
- Cisco 827, 827H, 827-4V, and 837
- Cisco SOHO 77, SOHO 77H, SOHO 78, SOHO 96, and SOHO 97
- Cisco 828

The PPPoE client is supported on an ATM permanent virtual circuit (PVC). Only one PPPoE client is supported on a single ATM PVC.

Follow these steps to configure the router for PPPoE client support:

---

**Step 1** Configure the virtual private dialup network (VPDN) group number.

**a.** Enter the **vpdn enable** command in global configuration mode.

**b.** Configure the VPDN group by entering the **vpdn group** *tag* command.

**c.** Specify the dialing direction by entering the **request-dialin** command in the VPDN group.

**d.** Specify the type of protocol in the VPDN group by entering the **protocol pppoe** command.

**Step 2** Configure the ATM interface with PPPoE support.

**a.** Configure the ATM interface by entering the **interface atm 0** command.

**b.** Specify the ATM PVC by entering the **pvc** *number* command.

**c.** Configure the PPPoE client and specify the dialer interface to use for cloning by entering the **pppoe-client dial-pool-number** *number* command.

**Step 3** Configure the dialer interface by entering the **int dialer** *number* command.

**a.** Configure the IP address as negotiated by entering the **ip address negotiated** command.

**b.** (Optional) Configure authentication for your network by entering the **ppp authentication** protocol command.

**c.** Configure the dialer pool number by entering the **dialer pool** *number* command.

d. Configure the dialer-group number by entering the **dialer-group** *number* command.

e. Configure a dialer list corresponding to the dialer-group by entering the **dialer-list 1 protocol ip permit** command.

**Note** Multiple PPPoE clients can run on a different PVCs, in which case each client has to use a separate dialer interface and a separate dialer pool, and the PPP parameters need to be applied on the dialer interface.

A PPPoE session is initiated on the client side by the network. If the session has a timeout or is disconnected, the PPPoE client immediately attempts to reestablish the session.

If you enter the **clear vpdn tunnel pppoe** command with a PPPoE client session already established, the PPPoE client session stops, and the PPPoE client immediately tries to reestablish the session.

## Configuration Example

The following example shows a configuration of a PPPoE client.

```
vpdn enable
vpdn-group 1
    request-dialin
protocol pppoe

int atm0

pvc 1/100
    pppoe-client dial-pool-number 1

int dialer 1
ip address negotiated
ppp authentication chap
dialer pool 1
dialer-group 1
```

# Configuring TCP Maximum Segment Size for PPPoE

The configuring TCP maximum segment size for PPP over Ethernet feature is supported on the following Cisco routers:

- Cisco 806 and 831
- Cisco 826 and 836
- Cisco 827, 827H, 827-4V, and 837
- Cisco SOHO 77, SOHO 77H, SOHO 78, SOHO 96, and SOHO 97
- Cisco 828

If a Cisco router terminates the PPPoE traffic, a computer connected to the Ethernet interface may have problems accessing websites. The solution is to manually reduce the maximum transmission unit (MTU) configured on the computer by constraining the TCP maximum segment size (MSS). Enter the following command on the router’s Ethernet 0 interface:

```
ip tcp adjust-mss mss
```

where *mss* is 1452 or less.

## Configuration Example

The following example shows a configuration of a PPPoE client.

```
vpdn enable
no vpdn logging
!
vpdn-group 1
 request-dialin
  protocol pppoe
!
interface Ethernet0
 ip address 192.168.100.1 255.255.255.0
 ip tcp adjust-mss 1452
 ip nat inside
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 pvc 8/35
  pppoe-client dial-pool-number 1
```

```
!
dsl operating-mode auto
!
interface Dialer1
ip address negotiated
ip mtu 1492
ip nat outside
encapsulation ppp
dialer pool 1
dialer-group 1
ppp authentication pap callin
ppp pap sent-username sohodyn password 7 141B1309000528
!
ip nat inside source list 101 interface Dialer1 overload
ip route 0.0.0.0.0.0.0.0 Dialer1
access-list 101 permit ip 192.168.100.0.0.0.0.255 any
```

# Configuring Low Latency Queuing and Link Fragmentation and Interleaving

Low latency queuing (LLQ) provides a low-latency, strict-priority transmit queue for voice over IP (VoIP) traffic.

LLQ is supported on the following Cisco routers:

- Cisco 806
- Cisco 826 and 836
- Cisco 827, 827H, 827-4V, 831, and 837
- Cisco 828

Link fragmentation and interleaving (LFI) reduces voice traffic delay and jitter by fragmenting large data packets and interleaving voice packets within the data fragments.

## Configuring Low Latency Queuing

Follow the steps below to configure the router for LLQ :

**Step 1** Ensure that the voice and data packets have different IP precedence values so that the router can differentiate between them. Normally, data packets should have an IP precedence of 0, and voice packets should have an IP precedence of 5. If the VoIP packets are generated from within the router, you may set the IP precedence to 5 for these packets by entering the **ip precedence** *number* command in dial-peer voice configuration mode as follows:

a. Enter the global configuration **dial-peer voice** *1* **voip** command.

b. Enter the **ip precedence** *5* command.

**Step 2** Create an access list and a class map for the voice packets.

a. Create an access list by entering the **access-list** *101* **permit ip any any precedence** *5* command.

b. Create a class map for the voice packets by entering **class-map match-all voice** command.

c. Link the class map to the access list by entering the **match access-group** *101* command.

**Step 3** Create LLQ for voice traffic.

a. Create a policy map by entering the **policy-map** *mypolicy* command.

b. Define the class by entering the **class voice** command.

c. Assign the priority bandwidth to the voice traffic. The priority bandwidth assigned to the voice traffic depends on the codec used and the number of simultaneous calls that you allow. For example, a G.711 codec call consumes 200 kbps; therefore, to support one G.711 voice call you would enter a **priority** *200* command.

**Step 4** Attach LLQ to the dialer interface.

a. Enter the global configuration **interface dialer** *1* command.

b. Create a service policy by entering the **service-policy out** *mypolicy* command.

# Configuring LFI

Follow the steps below to configure the router for LFI.

**Note** When you are configuring LFI, the data fragment size must be greater than the voice packet size; otherwise, the voice packets fragment, and voice quality deteriorates.

**Step 1** Configure the dialer bandwidth. The dialer interface has a default bandwidth of 56 kbps, which may be less than the upstream bandwidth of your digital subscriber line (DSL) connection. You can find the upstream bandwidth of your DSL connection by entering the **show dsl interface atm0** command in dialer interface configuration mode. If you have two or more PVCs sharing the same DSL connection, the bandwidth configured for the dialer interface must be the same as the bandwidth allocated to its assigned PVC.

**Step 2** Enable PPP multilink, and configure fragment delay and interleaving for the dialer interface.

**a.** Enter the global configuration **interface dialer** *1* command.

**b.** Specify the dialer bandwidth by entering the **bandwidth** *640* command. The bandwidth is specified in kilobits per second (kbps).

**c.** Enter the **ppp multilink** command.

**d.** Specify PPP multilink interleaving by entering the **ppp multilink interleave** command.

**e.** Define the fragment delay by entering the **ppp multilink fragment-delay** *10* command.

**f.** Calculate the fragment size using the following formula:

fragment size = (bandwidth in kbps/ 8) * fragment-delay in milliseconds (ms)

In this case, the fragment size = (640/8) * 10, resulting in a fragment size of 800. The fragment size is greater than the maximum voice packet size of 200, which is G.711 20 ms. A low fragment delay corresponds to a fragment size that may be smaller than the voice packet size, resulting in reduced voice quality.

# Configuring Class-Based Traffic Shaping to Support Low Latency Queuing

Class-based traffic shaping (CBTS) is supported on the following Cisco routers:

- Cisco 806
- Cisco 831

CBTS can be used to control the WAN interface traffic transmission speed to match the speed of the attached broadband modem or of the remote target interface. CBTS ensures that the traffic conforms to the policies configured for it, thereby eliminating topology bottlenecks with data-rate mismatches.

The **shape average** *kbps* and the **shape peak** *kbps* commands enable you to define traffic shaping for an interface.

**Note** CBTS is supported on the Ethernet 1 interface.

## Configuring CBTS for LLQ

Follow the steps below to configure CBTS, beginning in global configuration mode. This procedure shows how to create multiple traffic classes and associate them with policy maps, and then to associate the policy maps with a router interface.

**Step 1** Define a traffic classification.

**a.** Enter the **class-map** *map-name* command to define a traffic classification. For example, the name *voice* could be used to specify that this is a class map for voice traffic.

**b.** Now in class configuration mode, enter the **match ip precedence 5** command to match all IP voice traffic with a precedence of 5. Cisco Architecture for Voice, Video and Integrated Data (AVVID) documentation specifies a precedence value of 5 for voice-over-IP traffic.

**c.** Enter **exit** to leave class configuration mode.

**Step 2** Define a policy map and associated classes for low-latency queuing.

a. Enter the **policy-map** *map-name* command in global configuration mode to construct policies and to allocate different network resources for the defined traffic classes. The name *LLQ* could be used to specify that this is the policy map for LLQ.

b. Now in policy-map mode, define a class to handle voice traffic by entering **class** *QOS-class-name*, using the class-map name you defined using the **class-map** command in Step 1. This command places the router in QOS-class configuration mode.

c. Enter **priority** *number,* where number is bandwidth in kilobits per second. A value of 300, as shown in the example configuration, provides enough bandwidth for two G.711 voice ports. Before setting a priority value, refer to the specification for the CODEC used for voice calls.

d. Enter **exit** to return to policy-map configuration mode.

e. Enter **class class-default** to use the default class for all traffic other than voice traffic. The name class-default is well known, and does not have to be predefined using the **class-map** command.

f. Apply WFQ to non-voice traffic by entering the **fair-queue** command.

g. Enter **exit** twice to return to global configuration mode.

**Step 3** Define a traffic-shaping policy map.

a. Enter **policy-map** *map-name* in global configuration mode. The name *shape* should be used to indicate this map defines overall traffic shaping that is compatible with the remote transmission rate bandwidth.

b. Enter **class class-default** to associate the default class with this policy map.

c. Set the transmission speed to be used after traffic shaping to match the speed of the broadband modem or remote interface by entering the **shape average** *kbps* command, where *kbps* is a value in kilobits per second.

**Caution** The transmission speed entered must be less than or equal to the TX bandwidth of the DSL or cable modem to which the router is attached. Specifying a value greater than the modem’s TX bandwidth will result in the modem’s becoming congested, and the benefits of applying QOS might be lost.

d. Enter **service-policy** *name* to associate the LLQ policy map with the traffic-shaping policy map. If the map name for the low-latency queue were *LLQ*, then *name* would be *LLQ*.

e. Enter **exit** twice to return to global configuration mode.

**Step 4** Apply these policies to the Ethernet 1 interface.

a. Enter the **interface Ethernet 1** command.

b. Apply the service policy to the Ethernet 1 interface by entering **service-policy output** *name*, where *name* matches the policy defined in the traffic-shaping policy map. If the traffic-shaping policy map name were *shape*, the service-policy name would also be *shape*.

**Step 5** Enter **end** to leave router configuration mode.

## Configuration Example

The following example shows how a Cisco 806 router can be configured to connect to a broadband modem with limited bandwidth, while ensuring voice line quality. Two policy maps are configured:

- Policy map *LLQ*
- Policy map *shape*

Policy map *LLQ* ensures that voice traffic has a strict priority queue with bandwidth of up to 300 kbps. The policy map shape limits the total throughput to 2.2 MBps.

```
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password encryption
!
hostname 806-uut
!
ip subnet-zero
!
class-map match-all voice
 match ip precedence 5
!
!
```

```
policy-map LLQ
  class voice
    priority 300
  class class-default
   fair-queue
policy-map shape
  class class-default
   shape average 2250000
   service-policy LLQ
!
interface Ethernet0
 ip address 1.7.65.11 255.255.0.0
!
interface Ethernet1
 ip address 192.168.1.101 255.255.255.0
service-policy output shape
!
ip classless
ip http server
ip pim bidir-enable
!
line con 0
 stopbits 1
line vty 0 4
 login
!
!
scheduler max-task-time 5000
end
!
```

# Configuring the Length of the PVC Transmit Ring

The length of the PVC transmit ring can be configured on the following Cisco routers:

- Cisco 826 and 836
- Cisco 827, 827H, 827-4V, and 837
- Cisco SOHO 77, SOHO 77H, SOHO 78, SOHO 96, and SOHO 97
- Cisco 828

If both voice and data packets share the same PVC, it is important to reduce the PVC transmit (TX) ring size. This reduces the maximum number of data packets and fragments that can be in front of a voice packet in the hardware queue, thus reducing latency.

Follow these steps to reduce the PVC TX ring size:

**Step 1** Enter the global configuration **int atm 0** command.

**Step 2** Specify the PVC number by entering the **pvc** *1/100* command.

**Step 3** Reduce the PVC TX ring size to 3 by entering the **tx-ring-limit** *3* command.

# Configuration Example

The following example combines LFI, LLQ, and the PVC TX ring configurations.

```
class-map match-all voice
match access-group 101
!
policy-map mypolicy
 class voice
  priority 200
 class class-default
  fair-queue
!
interface Ethernet0
ip address 70.0.0.1 255.255.255.0
no ip mroute-cache
!
interface ATM0
 no ip address
 bundle-enable
 dsl operating-mode auto
!
interface ATM0.1 point-to-point
 no ip mroute-cache
 pvc 1/40
 encapsulation aal5mux ppp dialer
 dialer pool-member 1
 tx-ring-limit 3
!
interface Dialer1
 bandwidth 640
 ip address 60.0.0.1 255.255.255.0
 encapsulation ppp
 dialer pool 1
 service-policy output mypolicy
 ppp multilink
 ppp multilink fragment-delay 10
 ppp multilink interleave
!
ip classless
no ip http server
!
access-list 101 permit ip any any precedence 5
!
voice-port 1
!
voice-port 2
!
voice-port 3
!
voice-port 4
dial-peer voice 110 pots
        destination-pattern 1105555
 port 1
!
dial-peer voice 210 voip
 destination-pattern 2105555
 session target ipv4:60.0.0.2
 codec g711ulaw
 ip precedence 5
```

# Configuring DHCP Server Import

The Cisco IOS DHCP server has been enhanced to allow configuration information to be updated automatically by PPP. You can enable PPP to automatically configure the Domain Name System (DNS), the Windows Information Name Server (WINS), or the NetBIOS Name Service (NBNS), and the server IP address information within a Cisco IOS DHCP server pool.

This feature is supported on the following Cisco routers:

- Cisco 806 and 831
- Cisco 826 and 836
- Cisco 827, 827H, 827-4V, and 837

- Cisco SOHO 77, SOHO 77H, SOHO 78, SOHO 91, SOHO 96 and SOHO 97
- Cisco 828

Follow the steps below to configure the Cisco router for DHCP server import:

**Step 1** Configure the asynchronous transfer mode (ATM) interface and the asymmetric digital subscriber line (ADSL) operating mode.

**Step 2** Create an ATM PVC for data traffic, enter virtual circuit configuration mode, and specify the virtual path identifier/virtual channel identifier (VPI/VCI) values, the encapsulation type, and the dial-pool member.

**Step 3** Create a dialer interface.

**a.** Enter configuration mode for the dialer interface.

**b.** Specify the MTU size as 1492.

**c.** Assign ***ip address negotiated*** to the dialer interface.

**d.** Configure the dialer group number.

**e.** Configure PPP encapsulation and (if needed) Challenge Handshake Authentication Protocol (CHAP).

**f.** Configure IP negotiation of DNS and WINS requests.

**Step 4** Define an IP DHCP pool name.

**a.** Configure the network and domain name (if needed) for the DHCP pool.

**b.** Enter the **import all** command.

**Step 5** Configure a dialer list and a static route for the dialer interface.

# Configuration Examples

The following example shows a configuration of the DHCP server import on the Cisco 800 series and Cisco SOHO series routers.

```
router-820#show run
Building configuration...
Current configuration :1510 bytes
version 12.1
no service single-slot-reload-enable
no service pad
```

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname router-820
logging rate-limit console 10 except errors
!
username 3620-4 password 0 lab
mmi polling-interval 60
mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
no ip finger
no ip domain-lookup
!
ip dhcp excluded-address 192.150.2.100
ip dhcp pool 2
import all
network 192.150.2.0 255.255.255.0
domain-name devtest.com
default-router 192.150.2.100
lease 0 0 3
!
no ip dhcp-client network-discovery
vpdn enable
no vpdn logging
vpdn-group 1
request-dialin
protocol pppoe

call rsvp-sync
!
interface Ethernet0
ip address 192.150.2.100 255.255.255.0
ip nat inside
!
interface ATM0
no ip address
no atm ilmi-keepalive
pvc 0/16 ilmi
!
pvc 1/40
protocol pppoe
pppoe-client dial-pool-number 1
!
bundle-enable
dsl operating-mode auto
```

```
!
interface Dialer0
ip address negotiated
ip mtu 1492
ip nat outside
encapsulation ppp
dialer pool 1
dialer-group 1
ppp authentication chap
ppp ipcp dns request
ppp ipcp wins request
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer0
no ip http server
!
ip nat inside source list 101 interface Dialer0 overload
access-list 101 permit ip any any
dialer-list 1 protocol ip list 101
snmp-server manager
!
voice-port 1
voice-port 2
voice-port 3
voice-port 4
!
line con 0
transport input none
stopbits 1
line vty 0 4
scheduler max-task-time 5000
end
```

The following example shows a DHCP proxy client configuration on the Cisco 800 series and Cisco SOHO series routers:

```
3620-4#show run
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 3620-4
logging rate-limit console 10 except errors
!
username 820-uut1 password 0 lab
username 820-uut4 password 0 lab
```

```
memory-size iomem 10
ip subnet-zero
!
no ip finger
!
ip address-pool dhcp-proxy-client
ip dhcp-server 192.150.1.101
vpdn enable
no vpdn logging
!
vpdn-group 1
accept-dialin
protocol pppoe
virtual-template 1
!
call rsvp-sync
cns event-service server
!
interface Ethernet0/0
ip address 192.150.1.100 255.255.255.0
half-duplex
!
interface Ethernet0/1
no ip address
shutdown
half-duplex
!
interface ATM1/0
no ip address
no atm scrambling cell-payload
no atm ilmi-keepalive
pvc 1/40
encapsulation aal5snap
protocol pppoe
!
interface Virtual-Template1
ip address 2.2.2.1 255.255.255.0
ip mtu 1492
peer default ip address dhcp
ppp authentication chap
!
ip kerberos source-interface any
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet0/0
no ip http server
!
dialer-list 1 protocol ip permit
dial-peer cor custom
```

```
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 0 4
login
end
```

The following example shows a configuration on the remote DHCP server on the Cisco 800 series and Cisco SOHO series routers.

```
2500ref-4#show run
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname 2500ref-4
!
no logging console
!
ip subnet-zero
no ip domain-lookup
ip host PAGENT-SECURITY-V3 45.41.44.82 13.15.0.0
ip dhcp excluded-address 2.2.2.1
!
ip dhcp pool 1
network 2.2.2.0 255.255.255.0
dns-server 53.26.25.23
netbios-name-server 66.22.66.22
domain-name ribu.com
lease 0 0 5
!
cns event-service server
!
interface Ethernet0
ip address 192.150.1.101 255.255.255.0
interface Ethernet1
ip address 192.168.254.165 255.255.255.0
interface Serial0
no ip address
shutdown
no fair-queue
interface Serial1
no ip address
```

```
shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 1.1.1.1
ip route 0.0.0.0 0.0.0.0 Ethernet0
no ip http server
!
dialer-list 1 protocol ip permit
line con 0
exec-timeout 0 0
transport input none
line aux 0
transport input all
line vty 0 4
login
no scheduler max-task-time
end
```

# Configuring IP Control Protocol Subnet Mask Delivery

The IP control protocol subnet mask delivery feature is supported on the following Cisco routers:

- Cisco 806
- Cisco 826 and 836
- Cisco 827, 827H, 827-4V, 831, and 837
- Cisco SOHO 77, SOHO 77H, SOHO 78, SOHO 91, SOHO 96, and SOHO 97
- Cisco 828

The IP Control Protocol (IPCP) feature assigns IP address pools to customer premises equipment (CPE) devices. These devices then assign IP addresses to the CPE and to a DHCP pool.

IPCP provides the following functions:

- The Cisco IOS CPE device requests and uses the subnet.
- The authentication, authorization, and accounting (AAA) Remote Authentication Dial-In User Service (RADIUS) provides the subnet and inserts the framed route into the proper virtual route forwarding (VRF) table.

- The provider edge or the edge router helps in providing the subnet through IPCP.

DHCP is no longer supported on the client side because the CPE can now receive both the IP address and the subnet mask during the PPP setup negotiation. If the CPE uses the DHCP servers to allocate addresses for its own network, subnets can be assigned through the node route processor (NRP) on the network access server (NAS) and distributed to the remote CPE DHCP servers.

Follow the steps below to configure the CPE for IPCP:

**Step 1** Configure the ATM interface, and enter the ADSL operating mode.

**Step 2** Configure the ATM subinterface.

**a.** Create an ATM PVC for data traffic, enter virtual circuit configuration mode, and specify the VPI and VCI values.

**b.** Set the encapsulation of the PVC as *aal5mux ppp* to support data traffic.

**Step 3** Create a dialer interface.

**a.** Enter configuration mode for the dialer interface.

**b.** Specify the PPP encapsulation type for the PVC.

**c.** Enter the **ip unnumbered Ethernet 0** command to assign the Ethernet interface to the dialer interface.

**d.** Configure the dialer group number.

**e.** Configure CHAP.

**f.** Enter the **ppp ipcp mask request** command.

**g.** Assign a dialer list to this dialer interface.

**Step 4** Define an IP DHCP pool name.

**a.** Enter the **import all** command.

**b.** Enter the **origin ipcp** command.

**Step 5** Configure the Ethernet interface, and assign an IP address pool. Enter the pool name that you defined in Step 4.

**Step 6** Configure a dialer list and a static route for the dialer interface.

# Configuration Examples

The following example shows a IPCP configuration on the Cisco 827-4V router:

```
router-8274v-1# show run
Building configuration...
Current configuration :1247 bytes
version 12.2
no service single-slot-reload-enable
no service pad
service timestamps debug datetime msec
service timestamps log uptime
no service password-encryption
!
hostname router-8274v-1
!
no logging buffered
logging rate-limit console 10 except errors
!
username 6400-nrp2 password 0 lab
ip subnet-zero
ip dhcp smart-relay
!
ip dhcp pool IPPOOLTEST
import all
origin ipcp
lease 0 0 1
!
no ip dhcp-client network-discovery
!
interface Ethernet0
ip address pool IPPOOLTEST
no shutdown
hold-queue 32 in
!
interface ATM0
no ip address
atm ilmi-keepalive
bundle-enable
dsl operating-mode auto
hold-queue 224 in
!
interface ATM0.1 point-to-point
pvc 1/40
no ilmi manage
encapsulation aal5mux ppp dialer
dialer pool-member 1
!
```

```
interface Dialer0
ip unnumbered Ethernet0
encapsulation ppp
dialer pool 1
dialer-group 1
no cdp enable
ppp authentication chap callin
ppp chap hostname router-8274v-1
ppp chap password 7 12150415
ppp ipcp accept-address
ppp ipcp dns request
ppp ipcp wins request
ppp ipcp mask request
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer0
no ip http server
!
dialer-list 1 protocol ip permit
!
line con 0
exec-timeout 0 0
stopbits 1
line vty 0 4
login
!
scheduler max-task-time 5000
end
```

The following example shows an IPCP configuration on the remote server for a Cisco 827-4V router:

```
6400-nrp2#show run
Building configuration...

Current configuration :1654 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 6400-nrp2
!
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa nas port extended
```

```
enable password lab
!
username router-8274v-1 password 0 lab
username TB2-8274v-2 password 0 lab
!
redundancy
main-cpu
auto-sync standard
no secondary console enable
ip subnet-zero
no ip finger
!
interface ATM0/0/0
no ip address
no atm ilmi-keepalive
hold-queue 500 in
!
interface ATM0/0/0.4 point-to-point
pvc 6/40
encapsulation aal5mux ppp Virtual-Template5
!
!interface ATM0/0/0.5 point-to-point
pvc 5/46
protocol ip 7.0.0.60 broadcast
encapsulation aal5mux ppp Virtual-Template6
!
interface Ethernet0/0/1
no ip address
shutdown
!
interface Ethernet0/0/0
description admin IP address 192.168.254.201 255.255.255.0
ip address 192.168.254.240 255.255.255.0
!
interface FastEthernet0/0/0
ip address 192.168.100.101 255.255.255.0
half-duplex
!
interface Virtual-Template5
ip unnumbered FastEthernet0/0/0
no keepalive
no peer default ip address
ppp authentication chap
!
interface Virtual-Template6
ip unnumbered FastEthernet0/0/0
no peer default ip address
ppp authentication chap
```

```
!
ip classless
no ip http server
!
ip radius source-interface FastEthernet0/0/0
!
radius-server host 192.168.100.100 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute nas-port format d
radius-server key foo
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 0 4
 password lab
!
end
```

The following example shows an IPCP configuration on the RADIUS server for a Cisco 827-4V router (Cisco Access Registrar 1.5):

```
/opt/AICar1/usrbin-4 % ./aregcmd
Access Registrar Configuration Utility Version 1.5
Copyright (C) 1995-1998 by American Internet Corporation, and
1998-2000 by
 Cisco Systems, Inc.  All rights reserved.
Cluster:localhost
User:admin
Password:
Logging in to localhost
400 Login failed/opt/AICar1/usrbin-5 % ./aregcmd
Access Registrar Configuration Utility Version 1.5
Copyright (C) 1995-1998 by American Internet Corporation, and
1998-2000 by
 Cisco Systems, Inc.  All rights reserved.
Cluster:localhost
User:admin
Password:
Logging in to localhost

[ //localhost ]
    LicenseKey = SBUC-7DQF-PM1E-5HPC (expires in 51 days)
    Radius/
    Administrators/

Server 'Radius' is Running, its health is 10 out of 10
```

```
--> cd radius

[ //localhost/Radius ]
    Name = Radius
    Description =
    Version = 1.6R1
    IncomingScript~ =
    OutgoingScript~ =
    DefaultAuthenticationService~ = local-users
    DefaultAuthorizationService~ = local-users
    DefaultAccountingService~ = local-file
    DefaultSessionService~ =
    DefaultSessionManager~ =
    UserLists/
    UserGroups/
    Policies/
    Clients/
    Vendors/
    Scripts/
    Services/
    SessionManagers/
    ResourceManagers/
    Profiles/
    Rules/
    Translations/
    TranslationGroups/
    RemoteServers/
    Advanced/
    Replication/

--> cd profile

[ //localhost/Radius/Profiles ]
ls
    Entries 1 to 6 from 6 total entries
    Current filter:<all>

    default-PPP-users/
    default-SLIP-users/
    default-Telnet-users/
    StaticIP/
    router-8274v-1/
    TB2-8274v-2/

--> ls

[ //localhost/Radius/Profiles ]
    Entries 1 to 6 from 6 total entries
    Current filter:<all>

    default-PPP-users/
    default-SLIP-users/
    default-Telnet-users/
    StaticIP/
    router-8274v-1/
    TB2-8274v-2/

--> cd router-8274v-1

[ //localhost/Radius/Profiles/router-8274v-1 ]
    Name = router-8274v-1
    Description =
    Attributes/

--> ls

[ //localhost/Radius/Profiles/router-8274v-1 ]
    Name = router-8274v-1
    Description =
    Attributes/

--> cd attribute

[ //localhost/Radius/Profiles/router-8274v-1/Attributes ]
    cisco-avpair = "ip:wins-servers=100.100.100.100 200.200.200.200"
    cisco-avpair = "ip:dns-servers=60.60.60.60 70.70.70.70"
    Framed-Compression = none
    Framed-IP-Address = 40.1.2.30
    Framed-IP-Netmask = 255.255.255.0
    Framed-MTU = 1500
    Framed-Protoc
l = ppp
    Framed-Routing = None
    Service-Type = Framed
```

# Configuring the Service Assurance Agent

The Service Assurance Agent (SAA) can be configured on the following Cisco routers:

- Cisco 806
- Cisco 826 and 836

- Cisco 827, 827H, 827-4V, 831, and 837
- Cisco SOHO 77, SOHO 77H, SOHO 78, SOHO 96, and SOHO 97
- Cisco 828

The SAA is an application-aware synthetic operation agent that monitors network performance by measuring key metrics such as response time, availability, jitter (interpacket delay variance), connect time, throughput, and packet loss. This feature is intended to provide support for Service Level Agreement (SLA) reporting functionality of the Cisco VPN Solution Center, but it can also be used for troubleshooting, analysis before problems occur, and for designing future network topologies. Response Time Monitoring (RTM) functionality is supported.

For configuration information on this command, refer to the Cisco IOS Release 12.0 documentation set.

# Configuring Secure Shell

Secure Shell (SSH) is a protocol that provides a secure and remote connection to a router. SSH is available in two versions: SSH Version 1 and SSH Version 2. Only SSH Version 1 is available in the Cisco IOS software.

SSH is supported on the following Cisco routers:

- Cisco 806
- Cisco 826 and 836
- Cisco 827, 827H, 827-4V, 831, and 837
- Cisco 828
- Cisco SOHO 91, SOHO 96, and SOHO 97

For configuration information on this command, refer to the Cisco IOS Release 12.0 documentation set.

# Configuring IP Named Access Lists

IP named access lists are supported on the following Cisco routers:

- Cisco 806
- Cisco 826 and 836
- Cisco 827, 827H, 827-4V, 831, and 837
- Cisco SOHO 77, SOHO 77H, SOHO 78, SOHO 96, and SOHO 97
- Cisco 828

You can identify IP access lists with an alphanumeric string (name) instead of a number. When you use named access lists, you can configure more IP access lists in a router.

For configuration information on this command, refer to the Cisco IOS Release 12.0 documentation set.

# Configuring International Phone Support

Cisco 827-4V routers provide international phone support (H.323 only) for the following countries:

- Italy
- Denmark
- Australia

International phone support commands configure voice port settings and caller ID settings.

H.323 international phone support has been tested and verified to work with the following equipment identified for Italy and Denmark.

The following devices are supported in Italy:

- Telephones:
  - Siemens Gigaset 3015 Class Model
  - Telecom Italia MASTER s.p. LUPO VIEW
  - Alcatel Dial Face Mod. SIRIO 2000 Basic A

- Caller ID devices:
  - BRONDI INDOVINO
- Fax equipment:
  - Canon FAX-B155

The following devices are supported in Denmark:

- Telephones:
  - Tele Danmark dana classic
  - Tele Danmark Danafon Topas
- Caller ID devices:
  - DORO Danmark DOROX5

Follow the steps below to configure a voice port to support caller ID, international cadence, impedance, and ring frequency, starting in global configuration mode:

| | Command | Task |
|---|---|---|
| Step 1 | **voice-port** *number* | Enter voice-port configuration mode. |
| Step 2 | **cptone** *country-code* | Specify settings for call-progress tone, ring cadence, line impedance, and ring frequency. |
| Step 3 | **caller-id enable**<br>**caller-id alerting** *alerting-method* | Enable caller ID support, or enter the second command to enable caller ID support and to specify the alerting method. |
| Step 4 | **caller-id block** | Request blocking of the display of caller ID information at the far end of the call. |
| Step 5 | **end** | Exit router configuration mode. |

# Configuration Example

The following voice-port configuration example shows two voice ports configured for the progress tone and line characteristics for Denmark. Caller ID is enabled on both ports, and port 1 requests that caller ID information be blocked at the other end when a phone call originates from this port. The second port uses the line-reversal alerting method.

```
!
voice-port 1
 cptone dk
 caller-id enable
 caller-id block
 timeouts call-disconnect 0
!
voice-port 2
 cptone dk
 caller-id alerting line-reversal
 timeouts call-disconnect 0
```

# International Tone, Cadence, Ring Frequency, and Impedance Support

The default voice-port configuration for all voice ports specifies the U.S. country code, 600-ohm impedance, and 25-Hz ring frequency. Cisco IOS software supports commands for setting ring tone, cadence, frequency, and line impedance.

## Configuring a Regional Analog Voice Tone

Use the **cptone** command to specify a regional analog voice interface-related tone. Use the **no** form of this command to disable the selected tone.

**cptone** { **dk** | **it** | **au** }

**no cptone** { **dk** | **it** | **au** }

The following table shows what each code specifies.

| Code | Country | Parameters |
|---|---|---|
| **dk** | Denmark | POTS line type 2 (complex impedance), a-law encoding, OSI disconnect supervision, 25-Hz ringing frequency, 0 guard time |

| Code | Country | Parameters |
|---|---|---|
| **it** | Italy | POTS line type 2 (complex impedance), a-law encoding, OSI disconnect supervision, 25-Hz ringing frequency, 0 guard time |
| **au** | Australia | POTS line type 2 (complex impedance), a-law encoding, OSI disconnect supervision, 20-Hz ringing frequency, 0 guard time |

## Configuring an FXS Ring Cadence

Use the **ring cadence** command in voice-port configuration mode to specify the ring cadence for a Foreign Exchange Station (FXS) voice port. Use the **no** form of this command to restore the default value for this command.

```
ring cadence cadence
no ring cadence
```

The **ring cadence** command can take the following values.

| Value | Meaning |
|---|---|
| define | User-defined cadence |
| pattern01 | 2 seconds on, 4 seconds off |
| pattern02 | 1 second on, 4 seconds off |
| pattern03 | 1.5 seconds on, 3.5 seconds off |
| pattern04 | 1 second on, 2 seconds off |
| pattern05 | 1 second on, 5 seconds off |
| pattern06 | 1 second on, 3 seconds off |
| pattern07 | 0.8 second on, 3.2 seconds off |
| pattern08 | 1.5 seconds on, 3 seconds off |
| pattern09 | 1.2 seconds on, 3.7 seconds off |
| pattern10 | 1.2 seconds on, 4.7 seconds off |

| Value | Meaning |
|---|---|
| pattern11 | 0.4 second on, 0.2 second off, then<br>0.4 second on, 2 seconds off |
| pattern12 | 0.4 second on, 0.2 second off, then<br>0.4 second on, 2.6 seconds off |

## Configuring the FXS Voice Port Ring Frequency

To specify the ring frequency for a specified FXS voice port, use the **ring frequency** command in voice-port configuration mode. Use the **no** form of this command to restore the default value for this command.

```
ring frequency frequency
no ring frequency
```

To select the ring frequency, use the commands as follows.

| | |
|---|---|
| *25* | Specify a 25-Hz ring frequency. |
| *50* | Specify a 50-Hz ring frequency. |

## Configuring the Terminating Impedance

Use the **impedance** command in voice-port interface mode to specify the terminating impedance of a voice port interface. Use the **no** form of this command to restore the default value.

```
impedance {600c | 600r | 900c | 900r | complex1 | complex2 }
no impedance {600c | 600r | 900c | 900r | complex1 | complex2 }
```

The following table shows what each code specifies.

| Code | Impedance |
|---|---|
| 600c | 600-ohm complex |
| 600r | 600-ohm real |
| 900c | 900-ohm complex |
| 900r | 900-ohm real |

| | |
|---|---|
| complex1 | complex 1 |
| complex2 | complex 2 |

When using the **impedance** command, be aware of the following constraints:

- The **c600r** option selects the current POTS line type 0 implementation.
- The **900r** option selects the current POTS line type 1 implementation.
- The **600c**, **900c**, **complex1**, and **complex2** options select the current POTS line type 2 implementation.

# International Caller ID Support

Caller ID (CLID) is an analog service that displays the number of the calling line to the receiving line's terminal device when it receives a call. In some countries, CLID is called Calling Line Identity Presentation (CLIP). The Cisco router receives CLID data as a part of the H.225 Setup Message and transmits it to the terminal device, which can either be a CLID device or a telephone capable of showing CLID messages.

There are two types of CLID: Type I and Type II. Type I transmits the CLID information when the receiving phone is on hook. Type II transmits the CLID information when the receiving phone is off hook. Only type I CLID is supported in this release.

## Configuring the FXS Port for Caller ID

To allow the sending of caller ID information to the FXS voice port, use the **caller-id enable** voice-port configuration command. To disable the sending of caller ID information, use the **no** form of this command, which also clears all other caller ID configuration settings for the voice port.

```
caller-id enable
no caller-id enable
```

The country code specified in the **cptone** command must represent one of the countries for which caller ID is supported. Caller ID is disabled by default.

## Configuring Caller ID Alerting

Specify the caller ID alerting method and enable caller ID support by using the **caller-id alerting** voice-port configuration command. The **no** form of this command sets the caller ID alerting type to caller ID alerting ring type 1.

```
caller-id alerting { line-reversal | pre-ring | ring < 1 | 2 > }
no caller-id alerting { line-reversal | pre-ring | ring < 1 | 2 > }
```

Alerting methods are described in the following table.

| Alerting Method | Description |
|---|---|
| **line-reversal** | Use line-reversal alerting method. |
| **pre-ring** | Set a 250-millisecond pre-ring alerting method for caller ID information for on-hook (Type 1) caller ID at an FXS voice port. |
| **ring** < **1** \| **2** > | Set the ring-cycle method for receiving caller ID information for on-hook (Type 1) caller ID at an FXS voice port.<br>• If your telephone service provider specifies it, use this setting to provide caller ID alerting (display) after the first ring at the receiving station.<br>• If your telephone service provider specifies it, use this setting to provide caller ID alerting (display) after the second ring. |

The default alerting method is **ring 1**. If the country in which the router is installed uses a different alerting method, the appropriate alerting method must be configured. The **caller-id alerting ring** command can be used in countries using the BellCore/Telcordia standard. The **caller-id alerting line-reversal**, the **caller-id alerting pre-ring**, and **caller-id alerting** ring commands can be used in countries that do not use the BellCore/Telcordia standard.

The **caller-id alerting** command automatically enables caller ID support for the specific voice port.

## Configuring Caller ID Display Blocking

To request the blocking of the display of caller ID information at the far end of a call for calls originated at an FXS port, use the **caller-id block** voice-port configuration command at the originating Foreign FXS voice port. To allow the display of caller ID information, use the **no** form of this command.

```
caller-id block
no caller-id block
```

The default is no blocking of caller ID information.

**Note** The calling party information is included in the routed on-net call, as this information is often required for other purposes, such as billing and call blocking. The request to block display of the calling party information on terminating FXS ports is normally accepted by Cisco routers, but no guarantee can be made regarding the acceptance of the request by other equipment.

# Configuring Committed Access Rate

This feature is available on the following Cisco routers:

- Cisco 806
- Cisco 826 and 836
- Cisco 827, 827H, 827-4V, 831, and 837
- Cisco 828

Use the committed access rate (CAR) to limit bandwidth transmission rates to traffic sources and destinations and to specify policies for handling traffic that breaches the specified bandwidth allocations. To enable CAR, enter the **rate-limit** command while in ATM interface configuration mode.

## Configuration Example

The following example shows a CAR configuration:

```
interface ATM0.1 point-to-point
 mtu 576
 ip address 10.0.0.10 255.255.255.0
 rate-limit output 368000 2000 2000 conform-action set-dscp-transmit
40 exceed-action set-dscp-transmit 48
 pvc 0/33
  protocol ip 10.0.0.9 broadcast
  vbr-nrt 142 142 1
  encapsulation aal5snap
 !
```

# Configuring VPN IPSec Support Through NAT

This feature is available on the following Cisco routers:

- Cisco 806
- Cisco 826 and 836
- Cisco 827, 827H, 827-4V, 831, and 837
- Cisco SOHO 77, SOHO 78, SOHO 96, and SOHO 97
- Cisco 828

This feature includes client software that does not use Transmission Control Protocol (TCP) wrapping or User Datagram Protocol (UDP) wrapping. On Cisco routers, this feature allows the simultaneous use of multiple, PC-based IPSec clients on which IPSec packet wrapping is disabled or is not supported. When PCs connected to the router create an IPSec tunnel, network address translation (NAT) on the router translates the private IP addresses in these packets to public IP addresses. This NAT feature also supports multiple Point-to-Point Tunnel Protocol (PPTP) sessions, which may be initiated by PCs with PPTP client software.

You must enter the following command in global configuration mode for this feature to work:

**ip nat inside source list** *number* **interface BVI** *number* **overload**

# NAT Default Inside Server Enhancement

This feature is supported on the following Cisco routers:

- Cisco 806
- Cisco 831, 836, and 837
- Cisco SOHO 91, SOHO 96, and SOHO 97

The NAT command has been extended to allow you to specify an inside local address to receive packets that do not match criteria in other NAT statements in the configuration.

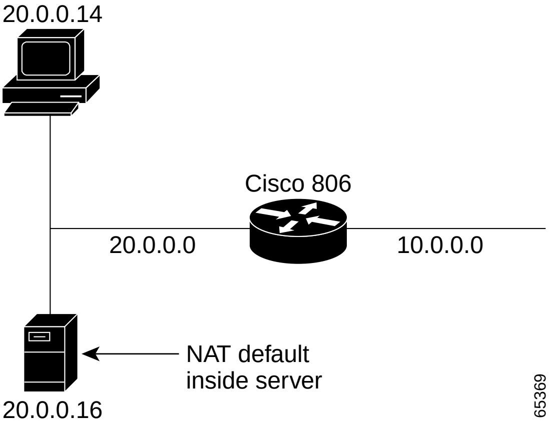
The syntax is as follows:

```
ip nat inside source static inside_local interface interface_name
```

# Configuration Example

The following example shows configuration of a Cisco 806 router supporting two devices with the addresses 20.0.0.14, and 20.0.0.16, as shown in Figure 8-1.

***Figure 8-1 Cisco 806 Router Performing Network Address Translation for Two Devices***



Several NAT statements direct traffic to the address 20.0.0.14. All packets not matching those NAT statements will be routed to 20.0.0.16.

```
Current configuration :942 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname c806-1
!
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto mib ipsec flowmib history tunnel size 200
crypto mib ipsec flowmib history failure size 200
!
interface Ethernet0
 ip address 20.0.0.1 255.0.0.0
 ip nat inside
 hold-queue 100 out
!
interface Ethernet1
 ip address 10.0.0.1 255.0.0.0
 ip nat outside
!
ip nat inside source static tcp 20.0.0.14 80 interface Ethernet1 80
ip nat inside source static udp 20.0.0.14 161 interface Ethernet1 161
!
ip nat inside source static 20.0.0.16 interface Ethernet1
! 20.0.0.16 is defined as the catch-all address
!
ip nat inside source static udp 20.0.0.14 1000 interface Ethernet1
1000
! udp port 1000 traffic will be routed to 20.0.0.14
!
ip nat inside source static tcp 20.0.0.14 23 interface Ethernet1 23
! telnet traffic will be routed to 20.0.0.14
!
ip classless
no ip http server
!
!
line con 0
```

```
 stopbits 1
line vty 0 4
 password lab
 login
!
```

# Configuring VoAAL2 ATM Forum Profile 9 Support

The Cisco 827-4V router supports voice over ATM Adaptation Layer 2 (VoAAL2) ATM Forum Profile 9. ATM Forum Profile 9 supports a 44-byte payload, optimizing voice transport efficiency, and makes interoperability with Tdsoft gateways possible.

This feature enables the Cisco router to interoperate with GR.303 and V5.2 gateways that communicate with Class 5 switches. The voice PVC is routed to a VoAAL2 gateway that supports either the General Recommendation 303 (GR.303) or the V5.2 protocol. This gateway converts the AAL2-encoded voice cells to a format that can be sent over a time-division multiplexed connection to a Class 5 switch. The data PVC can be routed through the digital subscriber line access multiplexer (DSLAM) or aggregator to the data network.

## Configuring ATM Forum Profile 9

Follow the steps below to configure ATM Forum Profile 9 support for a voice port, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **voice class permanent 1** | Configure a voice class. |
| Step 2 | **signal timing oos timeout disabled** | Disable the assertion of the receive out-of-service (oos) pattern to the PBX when signaling packets are lost. |
| Step 3 | **exit** | Exit voice class configuration mode. |
| Step 4 | **voice service voatm** | Enter voice service configuration mode. |
| Step 5 | **session protocol aal2** | Enter voice-service session configuration mode, and specify AAL2 trunking. |

| | Command | Task |
|---|---|---|
| Step 6 | **mode bles** | Indicate that VOATM is to be used in broadband loop emulation service (BLES) mode. |
| Step 7 | **exit** | Enter the **exit** command to leave session protocol mode. Enter **exit** again to leave voice service configuration mode. |
| Step 8 | **interface atm0** | Enter ATM 0 interface configuration mode. |
| Step 9 | **pvc** *vpi vci* | Specify the virtual path identifier (VPI) and the virtual channel identifier (VCI) of the PVC. |
| Step 10 | **vbr-rt** *pcr acr bcs* | Specify the variable bit rate-real time peak cell rate and average cell rate in kbps, and the burst cell size in number of cells. |
| Step 11 | **encapsulation aal2** | Specify ATM adaptation layer 2 (AAL2) type encapsulation. |
| Step 12 | **no atm cell-clumping-disable** | Ensure that sufficient bandwidth is allocated for data packets when voice calls are in progress. |
| Step 13 | **exit** | Exit ATM 0 interface configuration mode. |
| Step 14 | **dial-peer voice** *tag* **voatm** | Place the router in dial-peer voice configuration mode. |
| Step 15 | **session protocol aal2-trunk** | Configure the session protocol to support AAL2-trunk permanent (private line) trunk calls. |
| Step 16 | **session target atm0 pvc** *vpi/vci* **cid** *cid* | This command has three parameters: *vpi (*virtual path identifier), *vci* (virtual channel identifier), and *cid (*AAL2 channel identifier). |
| Step 17 | **codec aal2 profile** | Enter **codec aal2-profile atmf 9 g711alaw** to specify that only G.711 a-law is used for voice dial peer. Enter **codec aal2-profile atmf 9 g711ulaw** to specify that only G.711 mu-law is used for voice dial peer. |

| | Command | Task |
|---|---|---|
| Step 18 | **destination-pattern** *destination string* | Associate a dial-peer with a voice port. The *destination string* is the phone number in E.164 format that must match the destination string configured for the voice-port. |
| Step 19 | **voice-class permanent 1** | Associate this dial peer with the configured voice class. |
| Step 20 | **no vad** | Specify no voice activity detection (VAD). |
| Step 21 | **exit** | Exit dial peer voice configuration mode. |
| Step 22 | **voice port** *#* | Enter voice port configuration mode. |
| Step 23 | **connection trunk** *destination-pattern* | Specify the dialer string. The destination pattern must match the *destination-string* configured for the dial peer. |
| Step 24 | **playout-delay mode fixed no-timestamps** | Play out the AAL2 packet at a fixed rate, and ignore the time stamps carried in the packet. |
| Step 25 | **end** | Exit router configuration mode. |

**Note** One phone line requires a minimum setting of 78 kbps for both peak cell rate (PCR) and allowed cell rate (ACR) values.

# Configuration Example

The following example shows the configuration for two voice ports using Profile 9, and the G.711 a-law codec. VBR-RT, PCR, and ACR values are 312 to accommodate four phone lines, although only two phone lines are currently configured.

```
voice service voatm
 !
 session protocol aal2
  mode bles
!
!
voice class permanent 1
 signal timing oos timeout disabled
```

```
!
interface atm 0
 no atm cell-clumping-disable
 pvc 1/100
 vbr-rt 312 312 32
 encapsulation aal2
!
voice-port 1
 playout-delay mode fixed no-timestamps
 cptone DK
 timeouts wait-release 3
 connection trunk 8881052
 caller-id enable
 !
voice-port 2
 playout-delay mode fixed no-timestamps
 cptone DK
 timeouts wait-release 3
 connection trunk 8881053
 caller-id enable
!
!dial-peer voice 1000 voatm
 destination-pattern 8881052
 voice-class permanent 1
 session protocol aal2-trunk
 session target ATM0 pvc 1/100 16
 codec aal2-profile ATMF 9 g711alaw
 no vad
!
dial-peer voice 1001 voatm
 destination-pattern 8881053
 voice-class permanent 1
 session protocol aal2-trunk
 session target ATM0 pvc 1/100 17
 codec aal2-profile ATMF 9 g711alaw
 no vad
!
```

# Configuring ATM OAM F5 Continuity Check Support

This feature is available on the following Cisco routers:

- Cisco 826 and 836
- Cisco 827, 827H, and 837
- Cisco SOHO 77, SOHO 96, and SOHO 97

ATM Operation, Administration, and Maintenance (OAM) F5 continuity check (CC) cells enable network administrators to detect misconfigurations in the ATM layer. Such misconfigurations can cause misdelivery of a cell stream to a third party or can cause unintended merging of cells from multiple sources.

CC cells provide an in-service tool optimized to detect connectivity problems at the ATM layer. CC cells are sent between a router designated as the source location and a router designated as the sink location. The local router can be configured as the source, as the sink, or as both the source and the sink. It is not necessary to enter a CC configuration on the router at the other end of the segment, because the router on which CC has been configured sends a CC activation request to the router at the other end of the segment, directing it to act as either a source or a sink.

## Configuring Continuity Checking on a PVC

Use the following command to configure continuity checking on a PVC.

```
oam-pvc manage cc segment direction [ source | sink | both ]
```

Use the **no** form of this command to disable continuity checking on the segment.

```
no oam-pvc manage cc segment direction [ source | sink | both ]
```

### Configuration Example

The following configuration example activates CC over the segment and causes the router to function as the source.

```
interface ATM0
 ip address 10.0.0.3 255.255.255.0
 pvc 0/33
```

```
  oam-pvc manage cc segment direction source
 !
 end
```

The following configuration example activates CC over the segment and causes the router to function as the sink.

```
interface ATM0
 ip address 10.0.0.3 255.255.255.0
 pvc 0/33
  oam-pvc manage cc segment direction sink
 !
 end
```

The following configuration example activates CC over the segment and causes the router to function both as the source of CC cells and as the sink:

```
interface ATM0
 ip address 10.0.0.3 255.255.255.0
 pvc 0/33
  oam-pvc manage cc segment direction both
 !
 end
```

The following configuration example deactivates segment CC:

```
interface ATM0
 ip address 10.0.0.3 255.255.255.0
 pvc 0/33
    no oam-pvc manage cc
!
end
```

# Configuring CC Activation and Deactivation Request Frequency

The following command sets the frequency at which CC activation and deactivation requests are sent to the router at the other end of the segment.

**oam retry cc activation-count** *number* **deactivation-count** *number* **retry-frequency** *seconds*

The **no** form of this command removes these settings.

**no oam retry cc activation-count** *number* **deactivation-count** *number* **retry-frequency** *seconds*

### Configuration Example

The following configuration example sets the CC activation and deactivation counts, as well as the retry frequency:

```
interface ATM0
 ip address 10.0.0.3 255.255.255.0
 pvc 0/33
  oam-pvc manage cc segment direction source
  retry activation-count 10 deactivation-count 10 retry-frequency 3
 !
 end
```

## Disabling CC Support on the VC

The following command disables CC support on the virtual circuit (VC) under which the command has been entered. A PVC on which CC support has been disabled will deny CC activation requests.

**oam-pvc manage cc deny**

The **no** form of this command reenables CC support on the VC.

**no oam-pvc manage cc deny**

### Configuration Example

The following configuration example denies segment CC:

```
interface ATM0
 ip address 10.0.0.3 255.255.255.0
 pvc 0/33
    oam-pvc manage cc deny
 !
 end
```

## Configuring Continuity Checking Debugging

Use the following command to see the results of continuity checking.

```
debug atm oam cc interface atm number
```

The **no** form of this command disables continuity checking debugging.

```
no debug atm oam cc interface atm number
```

## Configuring Generation of End-to-End F5 OAM Loopback Cells

Follow the steps below to configure generation of an end-to-end F5 OAM loopback cell, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| Step 1 | **interface atm** 0 | Enter configuration mode for the ATM interface. |
| Step 2 | **pvc** routerA *vpi/vci* | Assign PVC to the name router A with the *vpi* and *vci* values. |
| Step 3 | **oam-pvc manage** *3* | Enable OAM management with a frequency of 3 seconds between OAM cell transmissions. |
| Step 4 | **oam retry** *5 5 10* | Configure the up count, down count, and retry frequency. |

The following example enables OAM management on an ATM PVC. The PVC is assigned the name router A and the VPI and VCI are assigned 0 and 32, respectively. OAM management is enabled with a frequency of 3 seconds between OAM cell transmissions.

```
interface atm 2/0
pvc routerA 0/32
oam-pvc manage 3
oam retry 5 5 10
```

## Example Output

The following example output of the debug **atm oam cc** command records activity beginning with the entering of the **oam-pvc manage cc** command, and ending with the entering of the **no oam-pvc manage cc** command. The ATM 0 interface is specified, and the “both” segment direction is specified. The output shows an activation request sent and confirmed, a series of CC cells sent by the routers on each end of the segment, and a deactivation request and confirmation.

```
router#debug atm oam cc interface atm0
Generic ATM:
  ATM OAM CC cells debugging is on
router#
00:15:05: CC ACTIVATE MSG (ATM0) I:VCD#1 VC 1/40 OAM Cell Type:4 OAM
Type:8 OAM Func:1 Direction:3 CTag:5
00:15:05: CC ACTIVATE CONFIRM MSG (ATM0) O:VCD#1 VC 1/40 OAM Cell
Type:4 OAM Type:8 OAM Func:1 Direction:3 CTag:5
00:15:06: CC CELL (ATM0) O:VCD#1 VC 1/40 OAM Cell Type:4 OAM Type:1
00:15:07: CC CELL (ATM0) I:VCD#1 VC 1/40 OAM Cell Type:4 OAM Type:1 OAM Func:4
00:15:08: CC CELL (ATM0) O:VCD#1 VC 1/40 OAM Cell Type:4 OAM Type:1 OAM Func:4
00:15:09: CC CELL (ATM0) I:VCD#1 VC 1/40 OAM Cell Type:4 OAM Type:1 OAM Func:4
00:15:10: CC CELL (ATM0) O:VCD#1 VC 1/40 OAM Cell Type:4 OAM Type:1 OAM Func:4
00:15:11: CC CELL (ATM0) I:VCD#1 VC 1/40 OAM Cell Type:4 OAM Type:1 OAM Func:4
00:15:12: CC CELL (ATM0) O:VCD#1 VC 1/40 OAM Cell Type:4 OAM Type:1 OAM Func:4
00:15:13: CC CELL (ATM0) I:VCD#1 VC 1/40 OAM Cell Type:4 OAM Type:1 OAM Func:4
00:15:14: CC CELL (ATM0) O:VCD#1 VC 1/40 OAM Cell Type:4 OAM Type:1 OAM Func:4
00:15:15: CC CELL (ATM0) I:VCD#1 VC 1/40 OAM Cell Type:4 OAM Type:1 OAM Func:4
00:15:16: CC CELL (ATM0) O:VCD#1 VC 1/40 OAM Cell Type:4 OAM Type:1 OAM Func:4
00:15:17: CC CELL (ATM0) I:VCD#1 VC 1/40 OAM Cell Type:4 OAM Type:1 OAM Func:4
00:15:18: CC CELL (ATM0) O:VCD#1 VC 1/40 OAM Cell Type:4 OAM Type:1 OAM Func:4
00:15:19: CC CELL (ATM0) I:VCD#1 VC 1/40 OAM Cell Type:4 OAM Type:1 OAM Func:4
00:15:19: CC DEACTIVATE MSG (ATM0) I:VCD#1 VC 1/40 OAM Cell Type:4 OAM
Type:8 OAM Func:1 Direction:3 CTag:6
00:15:19: CC DEACTIVATE CONFIRM MSG (ATM0) O:VCD#1 VC 1/40 OAM Cell
Type:4 OAM Type:8 OAM Func:1 Direction:3 CTag:6
```

The following table describes significant fields.

| Field | Description |
|---|---|
| 00:15:05 | Time stamp. |
| CC ACTIVATE MSG (ATM0) | Message type and interface. |
| 0 | Source. |

| Field | Description |
|---|---|
| 1 | Sink. |
| VC 1/40 | Virtual circuit identifier. |
| Direction:3 | Indication of the direction in which the cells are traveling. 1 indicates local router operates as a sink. 2 indicates local router operates as a source. 3 indicates both routers operate as source and sink. |

# Configuring RADIUS Support

RADIUS is supported on the following Cisco routers:

- Cisco 806
- Cisco 826 and 836
- Cisco 827, 827H, 827-4V, 831, and 837
- Cisco 828

RADIUS enables you to secure your network against unauthorized access. A RADIUS server must be configured in the service provider or corporate network in order for the router to use RADIUS client features. For instructions on configuring RADIUS, refer to the *Cisco 806 Router Software Configuration Guide* and to the *Cisco IOS Security Configuration Guide*.

# Configuring Cisco Easy VPN Client

The Cisco Easy VPN Client feature is supported on the following Cisco routers:

- Cisco 806
- Cisco 826 and 836
- Cisco 827, 827H, 827-4V, 831, and 837
- Cisco 828

The Cisco Easy VPN client feature supports two modes of operation:

- Client—Specifies that Network Address Translation/Port Address Translation (NAT/PAT) be done, so that the PCs and other hosts at the client end of the VPN tunnel form a private network that does not use any IP addresses in the destination server's IP address space.
- Network Extension—Specifies that the PCs and other hosts at the client end of the VPN tunnel should be given IP addresses in the destination enterprise network's IP address space, so that they form one logical network.

Both modes of operation also optionally support split tunneling, which allows secure access to corporate resources through the VPN tunnel while also allowing Internet access through a connection to an ISP or other service (thereby eliminating the corporate network from the path for Web access). This configuration is enabled by a simple access list implemented on the IPSec server.

**Note** Cisco 800 series routers are supported as IPSec clients of VPN 3000 concentrators. Support for other IPSec servers will be available in a future release. Be sure to refer to the Cisco IOS release notes for the current release to determine if there are any other limitations on the use of Cisco Easy VPN Client.

The release note *Cisco EZVPN Client for the Cisco uBR905/uBR925 Cable Access Routers* provides instructions for configuring the DHCP server pool and the Easy VPN client profile required for implementing Easy VPN. The release note also provides configuration examples for the IPSec server and descriptions of commands for managing Easy VPN.

# Configuration Example

This section provides a client mode configuration example for the Cisco 827 router.

The following example configures a Cisco 827 router as an IPSec client, using the Cisco Easy VPN feature in the client mode of operation. This example shows the following components of the Cisco Easy VPN client configuration:

- DHCP server pool—The **ip dhcp pool** command creates a pool of IP addresses to be assigned to the PCs connected to the router's Ethernet 1 interface. The pool assigns addresses in the class C private address space

(192.168.100.0) and configures each PC so that its default route is 192.168.100.1, which is the IP address assigned to the router’s Ethernet interface.

- EzVPN client configuration—The first **crypto ipsec client ezvpn hw-client** command (global configuration mode) creates an EzVPN client configuration named *hw-client*. This configuration specifies a group name of *hw-client-groupname* and a shared key value of *hw-client-password*, and it sets the peer destination to the IP address **188.185.0.5** (which is the address assigned to the interface connected to the Internet on the destination peer router). The EzVPN configuration is configured for the default operations mode **client**.

**Note** If DNS is also configured on the router, the **peer** option also supports a host name instead of an IP address.

- The second **crypto ipsec client ezvpn hw-client** command (ATM 0 interface configuration mode) assigns the EzVPN client configuration to the ATM 0 interface, so that all traffic received and transmitted on that interface is sent through the VPN tunnel.

The following is an example output of the **show running-config** command:

```
Current configuration :1040 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname c827-18
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip dhcp excluded-address 192.168.100.1
!
ip dhcp pool CLIENT
 import all
 network 192.168.100.0 255.255.255.0
 default-router 192.168.100.1
```

```
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto ipsec client ezvpn hw-client
 group hw-client-groupname key hw-client-password
 mode client
 peer 188.185.0.5
!
interface Ethernet0
 ip address 192.168.100.1 255.255.255.0
 hold-queue 100 out
!
interface ATM0
 ip address 192.168.101.18 255.255.255.0
 no atm ilmi-keepalive
  protocol ip 192.168.101.19 broadcast
  encapsulation aal5snap
 !
 dsl operating-mode auto
 crypto ipsec client ezvpn hw-client
!
ip classless
ip route 0.0.0.0 0.0.0.0 ATM0
ip route 50.0.0.0 255.0.0.0 40.0.0.19
ip http server
ip pim bidir-enable
!
line con 0
 stopbits 1
line vty 0 4
 login
!
```

# Configuring Dial-on-Demand Routing for PPPoE Client

Dial-on-demand routing (DDR) for PPPoE client is supported on the following Cisco routers:

- Cisco 806
- Cisco 826 and 836
- Cisco 827, 827H, 827-4V, 831, and 837

- Cisco SOHO 77, SOHO 77H, SOHO 78, SOHO 91, SOHO 96, and SOHO 97
- Cisco 828

DDR for the PPPoE client provides flexibility for subscribers whose ISP charges are based on the amount of time that they are connected to the network (non-flat-rate services). With the DDR for PPPoE client feature, you can designate a type of traffic as traffic of interest. You can then configure the router so that it will bring up the PPPoE connection when any traffic of interest arrives from the LAN interface and so that it will bring down the connection when the dialer idle timer expires.

DDR is configured in Ethernet 1 configuration mode, using the **pppoe-client dial-pool-number command** with the **dial-on demand** keyword. The syntax is shown below.

```
pppoe-client dial-pool-number number [dial-on-demand]
```

## Configuring DDR for a PPPoE Client

Follow the steps below to configure DDR for a PPPoE client, beginning in global configuration mode:

**Step 1** Enable VPDN.

a. In global configuration mode, enter the **vpdn enable** command.

b. Enter **no vpdn logging** command to disable vpdn logging.

**Step 2** Configure a virtual private dial-up network (VPDN) group.

a. Enter the global configuration mode **vpdn-group** *number* command, to enter vpdn group configuration mode.

b. Enter **request-dialin** to specify the dial-in dialing mode.

**Step 3** Configure the Ethernet 1 interface.

a. Enter **interface Ethernet 1** to enter Ethernet 1 interface configuration mode.

b. Enter **pppoe enable** to enable PPPoE for this interface.

c. Activate DDR and create a dial pool by entering **pppoe-client dial-pool-number** *number* **dial-on-demand**. The *number* value must match the vpdn group number.

**Step 4** Configure the dialer interface.

a. Enter **interface dialer 1** to enter dialer interface configuration mode.

b. Enter **ip address negotiated** to indicate that the ip address will be negotiated with the DHCP server.

c. Specify the maximum transmission unit size by entering **ip mtu 1492**.

d. Set the encapsulation type by entering **encapsulation ppp.**

e. Enter the **dialer pool** *number* command to associate the dialer interface with the dialer pool created for the Ethernet 1 interface.

f. Set the idle timer interval by entering **dialer idle-timeout 180 either**. The **either** keyword specifies that either inbound or outbound traffic can reset the idle timer.

**Note** A value of 0 specifies that the timer will never expire and that the connection will always be up.

g. Enter **dialer hold-queue 100** to set the queue to a size that will hold packets of interest before the connection is established.

h. Enter **dialer-group 1** to specify the dialer list that defines traffic of interest.

i. Leave Dialer 1 interface configuration mode by entering **exit**.

**Step 5** In the global configuration mode, enter the **dialer-list 1 protocol ip permit** command to define IP traffic as the traffic of interest.

**Step 6** Create a static route for the Dialer 1 interface by entering the **ip route 0.0.0.0 0.0.0.0 dialer 1 permanent** command.

**Step 7** Enter **end** to leave configuration mode.

# Configuring Weighted Fair Queuing

Weighted fair queuing (WFQ) is supported on the following Cisco routers:

- Cisco 806
- Cisco 826 and 836
- Cisco 827, 827H, 827-4V, 831, and 837 routers
- Cisco 828

WFQ has certain limitations. It is not scalable if the flow amount increases considerably, and native WFQ is not available on high-speed interfaces such as ATM interfaces. Class-based WFQ, available on Cisco IOS Plus images, overcomes these limitations.

## Configuring WFQ

Follow the steps below to apply WFQ to the ATM interface of a Cisco router.

**Step 1** Create a policy map for WFQ.

a. In global configuration mode, enter the **policy-map** *map-name* command to construct a WFQ policy. The map name *wfq* could be used to specify that this is the policy map for WFQ.

b. Enter **class class-default** to use the default class for all traffic.

c. Apply WFQ to all traffic by entering the **fair-queue** command.

d. Enter **exit** twice to return to global configuration mode.

**Step 2** Apply the policy map to the router interface.

a. Enter **interface atm** *number*, where *number* is the ATM interface number.

b. Enter **pvc** *vpi/vci* to specify which PVC you are applying the policy map to.

c. Enter **service-policy output** *map-name* to apply the policy to this PVC. If you named the policy map *wfq*, you would enter the command **service-policy output wfq**.

**Step 3** Enter **end** to leave router configuration mode.

# Example Configuration

The following configuration applies WFQ to PVC 0/33 on the ATM 0.1 interface. The policy map named *wfq* is created, and WFQ is applied to the default class referenced in that policy map. Then, *wfq* is referenced in the ATM 0.1 interface configuration.

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password encryption
!
hostname 806-uut
!
ip subnet-zero
!
policy-map wfq
  class class-default
  fair-queue
!
interface Ethernet0
ip address 192.168.1.1 255.255.255.0
!
interface atm0.1
 no ip address
 pvc 0/33
  service-policy output wfq
!
ip classless
ip http server
ip pim bidir-enable
!
line con 0
 stopbits 1
line vty 0 4
 login
!
scheduler max-task-time 5000
end
!
```

# Configuring DSL Commands

The sections below describe the supported DSL commands.

Follow the steps below to configure DSL command-line interface (CLI) commands.

| | Command | Task |
|---|---|---|
| Step 1 | **dsl noise-margin** | Set the noise margin offset. |
| Step 2 | **max-tone-bits** | Set the maximum bits per tone limit. |
| Step 3 | **gain-setting rx-offset** | Set the receive gain offset. |
| Step 4 | **gain-setting tx-offset** | Set the transmit gain offset. |

## Configuration Example

The following is a configuration example for the **dsl** command.

```
interface ATM0
 no ip address
 no atm ilmi-keepalive
 dsl operating-mode auto
 dsl noise-margin 0
 dsl max-tone-bits 14
 dsl gain-setting tx-offset 0
 dsl gain-setting rx-offset 1
```

# Enabling the DSL Training Log

The DSL training log feature is available on the following Cisco routers:

- Cisco 826 and 836
- Cisco 827, 827H, 827-4V, and 837 routers
- Cisco 828

By default, a DSL training log is retrieved each time the Cisco router establishes contact with the DSLAM. The training log is a record of the events that occur when the router *trains*, or negotiates communication parameters, with the DSLAM at the central office. However, retrieving this log adds significant amount of time to the training process, and retrieval is not always necessary after the router has successfully trained. You must use the **dsl enable-training-log** command to enable the retrieval of this log. The **no** form of this command disables retrieval of the DSL training log.

```
dsl enable-training-log
no dsl enable-training-log
```

## Retrieving the DSL Training Log and Then Disabling Further Retrieval of the Training Log

Complete the following tasks to retrieve the training log, examine it, and then disable the router from retrieving the training log the next time it trains with the DSLAM.

**Step 1** Configure the router to retrieve the training log.

a. Enter the global configuration mode **interface ATM** *number* command, where *number* is the number of the ATM interface.

b. Enter **dsl enable-training-log** to enable the retrieval of the training log**.**

c. Enter **end** to leave router configuration mode.

**Step 2** Unplug the DSL cable from the DSL socket on the back of the router, wait a few seconds, and then plug the cable back in.

**Step 3** When the “DSL line up” message appears, issue the **show dsl int atm** *number* command, where *number* is the number of the ATM interface, to display the retrieved log.

**Step 4** When you have decided that it is no longer necessary for the router to retrieve the training log, reconfigure the router to disable the retrieval of the log by completing the following tasks.

a. Enter the global configuration mode **interface ATM** *number* command, where *number* is the number of the ATM interface.

b. Enter **no dsl enable-training-log** to disable the retrieval of the training log.

c. Enter **end** to leave router configuration mode.

# Selecting Secondary DSL Firmware

This command is available on the Cisco 827, 827H, 827-4V, and 837 routers.

The ATM interface mode **dsl firmware secondary** command enables you to select the secondary DSL firmware.

```
dsl firmware secondary
```

To revert to using the primary firmware, enter the **no** form of this command.

```
no dsl firmware secondary
```

**Note** The router must retrain in order for the configuration changes to take effect. To retrain the line, you can unplug the DSL cable from the DSL socket on the back of the router and then plug the DSL cable back in again.

You can use the **show dsl interface atm** *number* command to compare firmware versions in use before retraining the DSL line, and after retraining.

## Output Example

The following example output contains **show dsl interface atm** command output before the **dsl secondary firmware** command is added to the configuration.

```
827-sus2#sh dsl int atm0
                 ATU-R (DS)                      ATU-C (US)
Modem Status:   Showtime (DMTDSL_SHOWTIME)
DSL Mode:       ITU G.992.1 (G.DMT)
ITU STD NUM:    0x01                            0x01
Vendor ID:      'ALCB'                          'GSPN'
Vendor Specific:0x0000                          0x0002
Vendor Country: 0x00                            0x00
Capacity Used:  66%                             74%
Noise Margin:   16.5 dB                         17.0 dB
Output Power:    8.0 dBm                        12.0 dBm
Attenuation:     0.0 dB                          4.0 dB
Defect Status:  None                            None
Last Fail Code: None
Selftest Result:0x49
Subfunction:    0x02
Interrupts:     652 (1 spurious)
Activations:    1
SW Version:     3.8129
```

```
FW Version:     0x1A04
```

After adding the **dsl firmware secondary** command to the configuration and retraining, the show dsl interface ATM0 output shows that the software version has changed to 3.7123.

```
827-sus2#sh dsl int atm0
                 ATU-R (DS)                      ATU-C (US)
Modem Status:   Showtime (DMTDSL_SHOWTIME)
DSL Mode:       ITU G.992.1 (G.DMT)
ITU STD NUM:    0x01                            0x01
Vendor ID:      'ALCB'                          'GSPN'
Vendor Specific:0x0000                          0x0002
Vendor Country: 0x00                            0x00
Capacity Used:  71%                             74%
Noise Margin:   18.0 dB                         17.0 dB
Output Power:    7.5 dBm                        12.0 dBm
Attenuation:     0.0 dB                          4.0 dB
Defect Status:  None                            None
Last Fail Code: None
Selftest Result:0x00
Subfunction:    0x02
Interrupts:     1206 (2 spurious)
Activations:    2
SW Version:     3.7123
FW Version:     0x1A04
```

## Configuration Example

The following example shows configuration of a Cisco 827 router using secondary DSL firmware.

```
827-sus2#sh run
Building configuration...

Current configuration :738 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
no service dhcp
!
hostname 827-sus2
!
ip subnet-zero
```

```
no ip domain-lookup
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
interface Ethernet0
 ip address 192.168.5.23 255.255.255.0
 no cdp enable
 hold-queue 100 out
!
interface Virtual-Template1
 ip address 2.2.3.4 255.255.255.0
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 pvc 1/40
  encapsulation aal5mux ppp Virtual-Template1
!
 dsl operating-mode itu-dmt
 dsl firmware secondary  ===========> New CLI
!
ip classless
ip http server
ip pim bidir-enable
!
line con 0
 exec-timeout 0 0
 stopbits 1
line vty 0 4
 login
!
scheduler max-task-time 5000
end

827-sus2#
```

# Configuring DNS-Based X.25 Routing

DNS-based X.25 routing is supported only on Cisco 805 routers.

The **x25 route** *disposition* **xot** command option has been modified to include the **dns** *pattern* argument after the **xot** keyword, where *pattern* is a rewrite element that works in the same way that address substitution utilities works.

# Configuring X.25 Load Balancing

X.25 load balancing is supported only on Cisco 805 routers. The Cisco 805 router supports only the rotary method of load distribution because it has only one serial interface.

The current X.25 allocation method for VCs across multiple serial lines fills one serial line to its VC capacity before utilizing the second line at all. As a result, the first serial line is frequently carrying its maximum data traffic before it runs out of VCs.

Using a facility called “hunt-group” (the method for X.25 load balancing), a switch can now view a pool of X.25 lines going to the same host as one address and can assign virtual circuits (VCs) on an “idle logical channel” basis. With this feature, X.25 calls can be load-balanced among all configured outgoing interfaces to fully use and balance all managed lines.

# Configuring X.25 Closed User Group

X.25 closed user group (CUG) is supported only on Cisco 805 routers.

A CUG is a collection of DTE devices for which the network controls access between two members and between a member and a non-member. An X.25 network can support up to 10,000 CUGs (numbered between 0 and 9999), each of which can have any number of member DTE devices. An individual DTE becomes a member of a specific network CUG by subscription. The subscription data includes the local number the DTE will use to identify the network CUG (which may or may not be the same as the network number, as determined by network administration and the DTE device’s requirements), and any restriction that prohibits the DTE from placing a call within the CUG or, conversely, prohibits the network from presenting a call within the CUG to the DTE.

CUGs are a network service to allow various network subscribers (DTE devices) to be segregated into private subnetworks with limited incoming or outgoing access, which means that a DTE must obtain membership from its network service (POP) for the set of CUGs it needs access to. A DTE may subscribe to none, one, or several CUGs at the same time. A DTE that does not require CUG membership for access is considered to be in the open part of the network. Each CUG typically permits subscribing users to connect to each other, but precludes connections with non-subscribing DTE devices.

# Configuring FTP Client

FTP client is available on all Cisco 800 series and Cisco SOHO 70 series routers except for the Cisco 801 through 804 routers.

FTP is an application protocol in the Internet protocol suite. It supports file transfers among unlike hosts in diverse internetworking environments. Using FTP, you can move a file from one computer to another, even if each computer runs a different operating system and uses a different file storage format. Cisco routers that can function as FTP clients can copy files from FTP servers into Flash memory.

When Cisco Router Web Setup (CRWS) software is installed on the router, it uses FTP to update the Cisco IOS image in Flash memory, and it configures the router with the FTP username and password that it requires.

⚠ **Caution** CRWS is unable to perform automatic updates if the FTP username and password values it places in the configuration file are changed.

If you need to use FTP to manually copy system images to Flash memory, see the instructions for adding an FTP username and password to the configuration file at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/ffcprt2/fcf008.htm

# Configuring Authentication Proxy

Authentication proxy is supported on Cisco 806 and 831 routers.

The Cisco IOS Firewall authentication proxy feature allows network administrators to apply specific security policies on a per-user basis. Previously, user identity and related authorized access was associated with a user's IP address, or a single security policy had to be applied to an entire user group or subnet. Now, users can be identified and authorized on the basis of their per-user policy, and access privileges tailored on an individual basis are possible, as opposed to general policy applied across multiple users.

With the authentication proxy feature, users can log into the network or access the Internet via HTTP. Their specific access profiles are automatically retrieved and applied from a Cisco Secure ACS or other RADIUS or TACACS+ authentication server. The user profiles are active only when there is active traffic from the authenticated users.

The authentication proxy is compatible with other Cisco IOS security features such as Network Address Translation (NAT), Context-based Access Control (CBAC), IP Security (IPSec) encryption, and VPN client software.

For instructions on configuring authentication proxy, refer to the *Cisco IOS Security Configuration Guide*.

# Configuring Port to Application Mapping

Port to Application Mapping (PAM) is supported on Cisco 806 and 831 routers.

PAM allows network administrators to customize network access control for specific applications and services.

PAM also supports host- or subnet-specific port mapping, which allows you to apply PAM to a single host or subnet, using standard access control lists (ACLs). Host or subnet specific port mapping is done using standard ACLs.

For instructions on configuring PAM, refer to the *Cisco IOS Security Configuration Guide*.

# Configuring CBAC Audit Trails and Alerts

Context-based Access Control (CBAC) audit trails and alerts are supported on Cisco 806 and 831 routers.

CBAC is a security feature that enables the router to filter TCP and UDP packets, based on application-layer protocol session information, and to generate real-time alerts and audit trails. Without CBAC, filtering can only be performed based on network layer and transport layer information. Enhanced audit trail features use SYSLOG to track all network transactions; recording time stamps, source host, destination host, ports used, and the total number of transmitted bytes, for advanced, session-based reporting. Real-time alerts send SYSLOG error messages to central management consoles upon detecting suspicious activity.

Using CBAC inspection rules, you can configure alerts and audit trail information on a per-application protocol basis. For example, if you want to generate audit trail information for HTTP traffic, you can specify that in the CBAC rule covering HTTP inspection.

For instructions on configuring CBAC audit trails and alerts, refer to the *Cisco IOS Security Configuration Guide*.

CHAPTER 9

# Troubleshooting

Use the information in this chapter to help isolate problems you might encounter with Cisco 800 series and Cisco SOHO series routers or to rule out the router as the source of the problem. This chapter contains the following sections:

Before troubleshooting a software problem, you must connect a terminal or PC to the router via the light-blue console port. (For information on making this connection, see the documentation listing in the "Related Documents" section on page xxxi.) With a connected terminal or PC, you can read 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

This section describes some asymmetric digital service line (ADSL) troubleshooting checks that you can perform if the router is not working properly. If you experience trouble with the ADSL connection, make sure to verify the following:

- That the ADSL line is connected and is using pins 3 and 4. For more information on the ADSL connection, refer to the hardware guide for your router.
- That the ADSL CD LED is on. If it is not on, the router may not be connected to the digital subscriber line access multiplexer (DSLAM). For more information on the ADSL LEDs, refer to the hardware installation guide specific to your router.
- That you are using the correct Asynchronous Transfer Mode (ATM) variable path indentifier/variable circuit identifier (VPI/VCI).
- That the DSLAM supports discrete multi-tone (DMT) Issue 2.

## ADSL Cable Requirements

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.

# G.SHDSL Troubleshooting

Symmetrical high-data-rate digital subscriber line (G.SHDSL) is available on Cisco 828 and Cisco SOHO 78 routers. This section describes some G.SHDSL troubleshooting checks that you can perform if the router is not working properly. If you experience trouble with the G.SHDSL connection, verify the following:

- That the G.SHDSL line is connected and is using pins 3 and 4. For more information on the G.SHDSL connection, refer to the *Cisco 828 Router and SOHO 78 Router Hardware Installation Guide*.
- That the G.SHDSL CD LED is on. If it is not on, the router may not be connected to the DSLAM. For more information on the G.SHDSL LEDs, refer to the *Cisco 828 Router and SOHO 78 Router Hardware Installation Guide.*
- That you are using the correct ATM VPI/VCI.
- That the DSLAM supports G.SHDSL.

## show dsl interface Command

Use the **show dsl interface** command to display the status of a G.SHDSL physical port on the router.

The following is an example of output for the **show dsl interface** command:

```
_Router# show dsl interface atm0

Globespan G.SHDSL/SDSL Chipset Information

 Equipment Type:          Customer Premise
 Operating Mode:          G.SHDSL Annex A
 Clock Rate Mode:         Fixed rate Mode
 Reset Count:             1
 Requested rate:          72 Kbps
 Actual rate:             72 Kbps
 Modem Status:            Data (0x1)
 Noise Margin:            37 dB
 Loop Attenuation:        0.4294963186 dB
 Transmit Power:          11.7 dBm
 Receiver Gain:           4.2040 dB (2271, 4210, 90)
 Last Activation Status: No Failure (0x0)
 CRC Errors:              2
 Chipset Version:         1
 Firmware Version:       R1.0
 Country Code:           0xB500
 Provider Code:          0x4E505347
 Vendor Data:            0x0 0x0 0x0 0x0
                         0x0 0x0 0x0 0x0

Performance statistics since reload:
Number of LOS failures:            0
Number of LOSQ failures:           0
Number of coding violations:       0
Number of errored seconds:         0
Number of severely errored seconds: 0
Number of unavailable seconds:     0

Performance statistics for:              Current 15 mins   Current 24
Hours
Time elapsed since beginning of interval:    6Min              0Hr
6Min
Number of LOS seconds:                       0                 0
Number of LOSQ seconds:                      0                 0
Number of code violations:                   0                 0
Number of errored seconds:                   0                 0
Number of severely errored seconds:          0                 0
Number of unavailable seconds:               0                 0
```

Table 9-1 describes possible command output for the **show dsl interface** command. Each line in the command output example corresponds to a row in this table.

*Table 9-1 show dsl interface Command Output Description*

| Output | Description |
|---|---|
| Equipment Type | • Customer premises equipment (CPE), if connected to a DSLAM.<br>• Central offices (COs); if the routers are connected back to back, then one of the routers can act as a CO. |
| Operating Mode | G.SHDSL annex configuration |
| Clock Rate Mode | Upstream and downstream bit rate configuration. Either AUTO for fixed. |
| Reset Count | Number of times the G.SHDSL chip has been reset since power-up. |

*Table 9-1 show dsl interface Command Output Description (continued)*

| Output | Description |
|---|---|
| Requested rate | User-specified bit rate requirement. |
| Actual rate | The actual bit rate that the transceiver is using. |
| Modem Status | • Handshake, when local transceiver tries to reach the far-end transceiver.<br>• Training; indicates that the startup training is in progress.<br>• Data, if successfully trained. |
| Received SNR | The received signal-to-noise ratio (SNR). |
| Loop Attenuation | The difference in decibels (dB) between the power received at the near-end and the power transmitted from the far-end. |
| Transmit Power | Local symmetric digital subscriber line transmission unit (STU) transmit power. |
| Receiver Gain | Total receiver gain. |
| Last Activation Status | Defines the last failure state of the G.SHDSL chip. |
| CRC Errors | Cyclic redundancy check (CRC) errors. |
| Chipset Version | Vendor’s chipset information. |
| Firmware Version | Vendor’s firmware release version. |
| Country Code | The country identification for the far end. |
| Provider Code | Identification of the vendor. |
| Vendor data | Vendor-specific information. |
| Number of LOS failures | Loss of synchronization counter increased when it contains one or more error in the framing bits. If the counter continues to increase during or after training, the line might be noisy or the cable is not connected. |
| Number of LOSQ failures | Loss of signal quality counter is increased when SNR is below the threshold. |

*Table 9-1 show dsl interface Command Output Description (continued)*

| Output | Description |
|---|---|
| Number of code violations | Code violation is defined as a count of the CRC anomalies occurring during the accumulation period. |
| Number of errored seconds | An errored second is a count of 1-second intervals during which one or more CRC anomalies/loss of sync words are declared. |
| Number of severely errored seconds | A severely errored second is a count of 1-second intervals during which 50 or more CRC anomalies are declared. |
| Number of unavailable seconds | An unavailable second is a count of 1-second intervals for which the DSL line is unavailable. |

# ATM Troubleshooting Commands

This section describes some ATM troubleshooting commands.

## ping atm interface Command

You can use the **ping atm interface** command to determine if a particular PVC is in use. The PVC does not need to be configured on the router in order for you to use this command.

For example, to test whether PVC 1/200 is in use, use the following command:

```
Router# ping atm interface atm 0 1 200 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 1 200 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 interface Command

Use the **show interface** command to display the status of all physical ports (Ethernet and ATM) and logical interfaces on the router. Significant messages in the command output are shown in bold. Significant messages are described in Table 9-2.

```
820-uut2#sh int atm0
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
820-uut2#sh int eth0
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)
820-uut2#sh int 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 9-2 describes possible command output for the **show interface** command. Each line in the command output example corresponds to a row in this table.

*Table 9-2 show interface Command Output Description*

| Output | Description |
|---|---|
| ATM0 is up, line protocol is up | • The ATM line is up and operating correctly. |
| **Other possible messages:** | |
| ATM0 is down, line protocol is down | • The ATM interface has been disabled with the **shutdown** command. |
| ATM0 is down, line protocol is down | • 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. |
| ATM0.1 is up, line protocol is up | • The first ATM subinterface is up and operating correctly. |
| **Other possible messages:** | |
| ATM0.1 is administratively down, line protocol is down | • The ATM subinterface has been disabled with the **shutdown** command. |
| ATM0.1 is down, line protocol is down | • The ATM subinterface is down, possibly because the ATM line has been disconnected (by the service provider). |

*Table 9-2 show interface Command Output Description (continued)*

| Output | Description |
|---|---|
| Ethernet0 is up, line protocol is up | • The Ethernet interface is connected to the network and operating correctly. |
| **Other possible messages:** | |
| Ethernet0 is up, line protocol is down | • The Ethernet interface has been correctly configured and enabled, but the Ethernet cable might be disconnected from the LAN. |
| Ethernet0 is administratively down, line protocol is down | • The Ethernet interface has been disabled with the shutdown command, and the interface is disconnected. |
| Dialer1 is up, line protocol is up | • Dialer1 is up and operating correctly. |
| **Another possible message:** | |
| Dialer1 is down, line protocol is down | • Dialer1 is not operating, possibly because the interface has been brought down with the shutdown command or the ADSL cable is disconnected. |
| Dialer1 is down, line protocol is down | • This is a standard message and does not indicate anything wrong with the configuration |

show atm interface Command

To display ATM-specific information about an ATM interface, use the **show atm interface atm0** privileged EXEC command. Following is the command syntax:

```
show atm interface atm0
```

The following is an example of output from the **show interface atm** command:

```
tw_820#sh atm int 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 9-3 describes the fields shown in the command output.

*Table 9-3 show atm interface Command Output Description*

| Field | Description |
|---|---|
| ATM interface | Interface number. Always 0 for the Cisco 827 routers. |
| AAL enabled | Type of AAL enabled. The Cisco 827 routers support AAL5. |
| 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 | The configured maximum number of bytes in the largest datagram. |
| PLIM Type | Physical layer interface module (PLIM) type |

# debug atm Commands

This section describes how to use the **debug atm** commands with additional keywords to troubleshoot the router.

## Before Using Debug Commands

You can use the debug commands to troubleshoot configuration problems that you might be having on your network. Debug commands provide extensive, informative displays to help you interpret any possible problems. All debug commands are entered in privileged EXEC mode, and most debug commands take no arguments. Read the information in Table 9-4 before using debug commands.

**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.

*Table 9-4 Important Information About Debug Commands*

| | |
|---|---|
| Additional documentation | You can find additional information and documentation about the debug commands in the *Debug Command Reference* document on the Cisco IOS software documentation CD-ROM that came with your router.<br>If you are not sure where to find this document on the CD-ROM, use the Search function in the Verity Mosaic browser that comes with the CD-ROM. |
| Disabling debugging | To turn off any debugging, enter the **undebug all** command. |
| Viewing debug message | To view debug messages on the console, enter the **logging console debug** command. |
| Telnet sessions | If you want to use debug commands during a Telnet session with your router, you must first enter the **terminal monitor** command. |

## debug atm errors Command

Use the **debug atm errors** command to display ATM errors. The **no** form of this command disables debugging output. Following is the command syntax:

```
debug atm errors
no debug atm errors
```

Following is sample **debug atm errors** output.

```
820-uut2#deb atm err
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 ATM events. The **no** form of this command disables debugging output. Following is the command syntax:

```
debug atm events
no debug atm events
```

This command displays ATM events that occur on the ATM interface processor and is useful for diagnosing problems in an ATM network. It provides an overall picture of the stability of the network.

If the interface is successfully communication with the DSLAM at the telephone company, the modem state is 0x10. If the interface is not communicating with the DSLAM, the modem state is 0x8.

The following output indicates that the ADSL line is up (training successful):

```
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]
```

In case of failure, you may see the modem state remain at 0x8 and not move to 0x10:

```
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 per-packet debugging output. The output reports information online when a packet is received or a transmission is attempted. The **no** form of this command disables debugging output. Following is the command syntax:

```
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]]
```

Following are the keywords used in this command:

| | |
|---|---|
| *interface atm number* | (Optional) ATM interface or subinterface number. |
| **vcd** *vcd-number* | (Optional) Number of the virtual circuit designator (VCD). |
| **vc** ***vpi/vci number*** | (Required) The vpi/vci value of the ATM PVC. |

The **debug atm packet** command displays all process-level ATM packets for both outbound and inbound packets. This command is useful for determining whether packets are being received and transmitted correctly.

**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.

Below is sample **debug atm packet** output.

```
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 9-5 describes the fields shown in the **debug atm packet** command output.

***Table 9-5 debug atm packet Command Output Description***

| Field | Description |
|---|---|
| ATM0 | Interface that is generating the packet. |
| (O) | Output packet. (I) would mean receive packet. |
| Pak size | Packet size in bytes. |
| 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. |
| DM: 0x*n* | Descriptor mode bits, where *n* is some value. |
| MUXETYPE: *n* | Multiplex type. |
| Length: *n* | Total length of the packet (in bytes) including the ATM header(s). |

# Troubleshooting Telephone Interfaces

Table 9-6 describes possible problems that your router might be experiencing and solutions for solving the problems. Table 9-7 describes the applicable debug commands.

***Table 9-6 Symptoms of Telephone Interfaces Trouble***

| Symptom | Possible Problem | Solution |
|---|---|---|
| Even though you have devices connected to ports 1 and 2, all calls are going to port 1. | You have not created dial peers. | Create dial peers. |
| You cannot make outgoing calls. | You have not specified all ISDN directory numbers with a SPID (North America only). | Check the settings of the **isdn spid 1** and **isdn spid 2** commands to make sure that you have specified all ISDN directory numbers for each SPID. |
| Even though you have created dial peers and set up distinctive ringing and ISDN voice priority, calls meant for secondary or tertiary ISDN directory numbers are routed to the primary number. | Incorrect dial peer, distinctive ringing, or ISDN voice priority configurations. | • Check dial peer, distinctive ringing, or ISDN voice priority configurations<br>• Use the **debug q931** command. |

*Table 9-7 Troubleshooting Telephone Interface*

| Command | Possible Problem | Solution |
|---|---|---|
| **debug pots driver** [**1** \| **2**] (privileged EXEC mode) | Caller ID device is not working either because you have not ordered the feature or because your device is not supported. | Contact your telephone service provider to verify that you ordered caller ID or to determine if there is a problem with the feature. |
| **debug pots csm** [**1** \| **2**] (privileged EXEC mode) | One of your dial peers might contain an invalid destination. | Check the settings of the destination pattern in each dial peer. If a setting is incorrect, use the **destination-pattern** *ldn* command. |

# Troubleshooting Serial Line Problems

This section describes how to troubleshoot problems in the following areas:

- Synchronous channel service unit/data service unit (CSU/DSU) clocking
- Synchronous leased lines
- Asynchronous dial-up lines
- Frame Relay
- X.25

## Synchronous CSU/DSU Clocking Problems

Clocking conflicts in serial connections can lead to either chronic loss of connection service or to degraded performance. This section describes how to detect and solve clocking problems with synchronous CSU/DSUs.

## Detecting Problems

Use the following steps to detect clocking conflicts on your serial interface:

**Step 1** Enter the **show interfaces serial 0** privileged EXEC command on the routers at both ends of the link.

**Step 2** Examine the output for cyclic redundancy check (CRC) or framing errors and aborts.

If the number of CRC or framing errors exceeds an approximate range of 0.5 to 2.0 percent of traffic on the serial interface, clocking problems are likely to exist somewhere in the WAN.

**Step 3** Isolate the source of the clocking conflicts by performing a series of ping tests and loopback tests (both local and remote).

**Step 4** Reenter the **show interfaces serial 0** privileged EXEC command on the routers at both ends of the link. Determine if CRC and framing errors are increasing and if so, where they are accumulating.

If input errors are accumulating on both ends of the connection, clocking of the CSU is the likely problem. If input errors are accumulating on one end of the connection, clocking of the DSU or cabling are the likely problems. If aborts are occurring on one end of the connection, the other end could be sending bad information or there could be a problem with the serial line.

Table 9-8 describes possible CSU/DSU clocking problems your router might be experiencing and the solutions for solving those problems.

*Table 9-8 Synchronous CSU/DSU Clocking Problems*

| Symptom | Solution |
|---|---|
| Incorrect CSU configuration | Perform the following tasks in the following order:<br>• Determine whether the CSUs at both ends of the serial line agree on the clock source (local or line).<br>• If the CSUs do not agree, configure them to do so.<br>• Check the line build out (LBO) setting on the CSU to ensure that the impedance matches that of the physical line. For information on configuring your CSU, refer to your CSU documentation. |
| Incorrect DSU configuration | Perform the following steps in the following order:<br>• Determine whether the DSUs at both ends of the serial line have serial clock transmit external (SCTE) mode enabled.<br>• If SCTE is not enabled on both ends of the connection, enable it.<br>• For any interface that is connected to a line of 128 kbps or faster, SCTE *must* be enabled.<br>• Make sure that ones density is maintained, which requires that the DSU use the same framing and coding schemes (for example, Extended Superframe Format [ESF] and Binary 8-Zero Substitution [B8ZS]) that are used by the leased line or other carrier service.<br>• Check with your leased line provider for information on its framing and coding schemes.<br>• If your carrier service uses Alternate Mark Inversion (AMI) coding, either invert the transmit clock on both sides of the link or run the DSU in bit-stuff mode. For information on configuring your DSU, refer to your DSU documentation. |

## Performing Ping Tests

Use the following steps to perform ping tests:

**Step 1** Put the CSU or DSU into local loopback mode.

**Step 2** Use the **ping** privileged EXEC command to send different data patterns and packet sizes.

## Performing Loopback Tests

These loopback tests do not apply to Frame Relay or X.25 networks.

### Local Loopback Tests

Follow the steps below to perform local loopback tests:

**Step 1** Place the CSU/DSU in local loop mode (refer to your CSU/DSU documentation).

In local loop mode, the use of the line clock (from the T1 service) is terminated, and the DSU is forced to use the local clock.

**Step 2** Enter the **show interfaces serial 0** privileged EXEC command to determine if the line status changes from “line protocol is down” to “line protocol is up (looped),” or if it remains down.

If the line protocol comes up when the CSU or DSU is in local loopback mode, a problem could be occurring on the remote end of the serial connection. If the status line does not change state, there is a possible problem in the router, connecting cable, or CSU/DSU.

If the problem appears to be local, enter the **debug serial interface** privileged EXEC command and go on to the next step.

**Step 3** Take the CSU/DSU out of local loop mode.

When the line protocol is down, the **debug serial interface** command output will indicate that keepalive counters are not incrementing.

**Step 4** Place the CSU/DSU in local loop mode again.

This action should cause the keepalive packets to begin to increment. Specifically, the values for *mineseen* and *yourseen* keepalives will increment every 10 seconds. This information will appear in the **debug serial interface** output.

If the keepalives do not increment, there may be a timing problem on the interface card or on the network.

**Step 5** Check the local router and CSU/DSU hardware, and any attached cables.

Make certain the cables are within the recommended lengths (no more than 50 feet [15.24 meters], or 25 feet [7.62 meters] for a T1 link). Make certain the cables are attached to the proper ports. Swap faulty equipment as necessary.

## Remote Loopback Tests

Follow the steps below to perform remote loopback tests:

**Step 1** Put the remote CSU or DSU into remote loopback mode (refer to the your CSU/DSU documentation).

**Step 2** Enter the **show interfaces serial 0** privileged EXEC command to determine if the line protocol remains up with the status line indicating “Serial *x* is up, line protocol is up (looped),” or if it goes down with the status line indicating “line protocol is down.”

If the line protocol remains up (looped), the problem is probably at the remote end of the serial connection (between the remote CSU/DSU and the remote router). Perform both local and remote tests at the remote end to isolate the problem source.

If the line status changes to “line protocol is down” when remote loopback mode is activated, make certain that ones density is being properly maintained. The CSU/DSU must be configured to use the same framing and coding schemes used by the leased-line or other carrier service (for example, ESF and B8ZS).

# Synchronous Leased Line Problems

Follow the steps below to troubleshoot problems with your synchronous leased line:

**Step 1** From privileged EXEC command mode, enter the **show interfaces serial 0** command.

If you see the line `Serial0 is up, line protocol is up`, the serial line is functioning properly. You do not need to take further action.

**Step 2** If you see one of the following messages, refer to Table 9-9:

- Serial 0 is down, line protocol is down.
- Serial 0 is up, line protocol is down.
- Serial 0 is up, line protocol is up (looped).
- Serial 0 is administratively down, line protocol is up.

*Table 9-9 Leased Line Problems*

| Line State | Problem | Solution |
|---|---|---|
| Serial 0 is down; line protocol is down. | The router is not sensing a carrier detect (CD) signal as a result of one of the following:<br>• Faulty or incorrect cabling of the router.<br>• Local router hardware failure.<br>• Local CSU/DSU hardware failure.<br>• WAN service provider problem, such as the line is down or not connected to the CSU/DSU. | Following are some steps you can take to isolate the problem:<br>• Refer to the *Cisco 805 Router Hardware Installation Guide* to confirm that you are using the correct serial cable to connect the CSU/DSU and that you connected the CSU/DSU correctly.<br>• Connect the leased line to another port, if possible. If the connection comes up, there is a hardware failure. Contact your Cisco reseller.<br>• Check the LEDs on the CSU/DSU for CD activity.<br>• Contact your WAN service provider. |

*Table 9-9 Leased Line Problems (continued)*

| Line State | Problem | Solution |
|---|---|---|
| Serial 0 is up; line protocol is down. | Possible causes for this line state are:<br>• Router hardware failure.<br>• Local or remote CSU/DSU hardware failure.<br>• Local or remote router misconfigured.<br>• The serial clock transmit external is not set on the CSU/DSU.<br>• The remote router is not sending keepalive packets.<br>• Problem with the leased line. | Following are some steps you can take to isolate the problem:<br>• Refer to the *Cisco 805 Router Hardware Installation Guide* to confirm that you are using the correct serial cable to connect the CSU/DSU and that you connected the CSU/DSU correctly.<br>• Connect the leased line to another port, if possible. If the connection comes up, there is a hardware failure. Contact your Cisco reseller.<br>• Check the LEDs on the CSU/DSU for CD activity.<br>• Perform CSU/DSU loopback tests. During local loopback, enter the **show interfaces serial 0** command. If the line protocol is shown as up, there might be a problem with the WAN service provider, or the remote router is down.<br>• Contact your WAN service provider. |

*Table 9-9 Leased Line Problems (continued)*

| Line State | Problem | Solution |
|---|---|---|
| Serial 0 is up;<br>line protocol is up (looped). | The possible cause is a loop in the circuit. The sequence number in the keepalive packet changes to a random number when a loop is first detected. If the same random number is returned over the line, a loop exists. | Following are some steps you can take to isolate the problem:<br>• Use the **write terminal** privileged EXEC command to display any instances of the loopback command. If the router has been configured with the loopback command, enter the **no loopback** command to remove the loop.<br>• Check to see whether the CSU/DSU is configured in manual loopback mode. If it is, disable manual loopback.<br>• Reset the CSU/DSU.<br>• If you are unable to isolate the problem, contact your WAN service provider for help with troubleshooting. |

*Table 9-9 Leased Line Problems (continued)*

| Line State | Problem | Solution |
|---|---|---|
| Serial 0 is administratively down; line protocol is up. | The possible causes for this state are:<br>• The serial interface has been disabled with the **shutdown** command.<br>• Different interfaces on the router are using the same IP address. | Following are some steps you can take to isolate the problem:<br>• Use the **show configuration** privileged EXEC command to display the serial port configuration. If "shutdown" is displayed after "interface Serial0," use the **no shutdown** command in serial interface configuration mode to enable the interface.<br>• Use the **show interface** privileged EXEC command to display the IP addresses for all router interfaces. Take the appropriate action to assign a unique IP address to each router interface. (If you set up your network per the sample networks in the this guide, refer to that particular sample network for information on how to assign a unique IP address to the router interfaces. |

# Asynchronous Dial-Up Problems

This section describes how to use the **show line 1** command to troubleshoot problems with the connection between your modem and router. It also describes the following symptoms, problems, and solutions:

- Troubleshooting Problems with Modem and Router Connection, page 9-26
- No Connectivity Between Modem and Router, page 9-28
- Modem Does Not Dial, page 9-29

## Troubleshooting Problems with Modem and Router Connection

Follow the steps below to troubleshoot problems with the connection between your modem and router:

**Step 1** In privileged EXEC command mode, enter the **show line 1** command.

Check the Modem state field in the output. If the modem state is Idle and CTS noDSR DTR RTS, the connection between your modem and router is functioning properly.

**Step 2** If you see one of the following modem states, see Table 9-10:

- Ready –
- Ready not CTS noDSR DTR RTS
- Ready CTS DSR DTR RTS
- Ready CTS* DSR* DTR RTS

*Table 9-10 Problems with Modem and Router Connection*

| Modem State | Problem |
|---|---|
| Ready – | • Modem control is not configured on the router. Enter the **modem inout** command in serial interface configuration mode.<br>• A session exists on the line. Enter the **show users** privileged EXEC command and the **clear line 0** privileged EXEC command to stop the session if desired.<br>• Data set ready (DSR) is high. There are two possible reasons for this:<br>– Cabling problems—If your modem connector uses DB-25 pin 6 and has no pin 8, you must move the pin from 6 to 8 or get the appropriate connector.<br>– Modem configured for data carrier detect (DCD) always high—The modem should be reconfigured to have DCD high only on carrier detect (CD), which is usually done with the **&C1** modem command. Check your modem documentation for the exact syntax for your modem.<br>• If your software does not support modem control, you must configure the router line to which the modem is connected with the no exec command in asynchronous line configuration mode. Clear the line with the clear line privileged EXEC command, initiate a reverse Telnet session with the modem, and reconfigure the modem so that DCD is high only on CD. End the Telnet session by entering disconnect and reconfigure the router line with the EXEC command in asynchronous line configuration mode. |
| Ready noCTS noDSR DTR RTS | • The modem is turned off.<br>• The modem is not properly connected to the router. Refer to the *Cisco 805 Router Hardware Installation Guide* for information on how to select the serial cable and how to connect the modem.<br>• The modem is not configured for hardware flow control. Disable hardware flow control on the router by entering the **no flowcontrol hardware** command in asynchronous line configuration mode. Enable hardware flow control on the modem via a reverse Telnet session. (Consult your modem documentation.) Reenable hardware flow control on the router by entering the **flowcontrol hardware** command in asynchronous line configuration mode. |

*Table 9-10 Problems with Modem and Router Connection (continued)*

| Modem State | Problem |
|---|---|
| Ready CTS DSR DTR RTS | • Incorrect cabling. Refer to the *Cisco 805 Router Hardware Installation Guide* for information on how to select the serial cable.<br>• The modem is configured for DCD always high. Reconfigure the modem so that DCD is only high on CD, which is usually done with the **&C1** modem command. Check your modem documentation for the exact syntax for your modem.<br>Configure the router line to which the modem is connected by entering the **no exec** command in asynchronous line configuration mode. Clear the line with the **clear line** privileged EXEC command, initiate a reverse Telnet session with the modem, and reconfigure the modem so that DCD is high only on CD. End the Telnet session by entering **disconnect**. Reconfigure the router line with the **exec** command in asynchronous line configuration mode. |
| **Note** Ready CTS* DSR* DTR RTS[1] | If this string appears in the Modem state field, modem control is probably not enabled on the router. Enter the **modem inout** command in asynchronous line configuration mode to enable modem control on the line. |

[1] An asterisk (*) next to a signal indicates one of two things: Either the signal has changed within the last few seconds, or the signal is not being used by the modem control method selected.

## No Connectivity Between Modem and Router

The connection between a modem and a Cisco router does not work. Attempts to initiate a reverse Telnet session to the modem have no result, or you receive a "Connection Refused by Foreign Host" message.

Table 9-11 outlines the problems that might cause this connectivity failure and describes possible solutions.

*Table 9-11 No Connectivity Between Modem and Router*

| Problem | Solution |
|---|---|
| Incorrect cabling. | Check the cabling between the modem and the router. Refer to the *Cisco 805 Router Hardware Installation Guide* for information on how to select the serial cable and how to connect the modem. |
| Hardware problem. | • Check the cabling between the modem and the router. Refer to the *Cisco 805 Router Hardware Installation Guide* for information on how to select the serial cable and how to connect the modem.<br>• Check all hardware for damage, including cabling (broken wires), adapters (loose pins), ports, and modem. |
| Modem control is not enabled on the router. | • Use the **show line 1** privileged EXEC command on the router. The output should show `inout` or `RIisCD` in the Modem column, which indicates that modem control is enabled on the line of the router.<br>• If necessary, configure modem control by using the **modem inout** command in asynchronous line configuration mode. |

## Modem Does Not Dial

Dial-up sessions cannot be established because the modem does not dial properly.

Table 9-12 outlines the problems that might cause this symptom and describes solutions to those problems.

*Table 9-12 Modem Does Not Dial*

| Problem | Solution |
|---|---|
| Incorrect cabling | Check the cabling between the modem and the router. Refer to the *Cisco 805 Router Hardware Installation Guide* for information on how to select the serial cable and how to connect the modem. |
| Modem hardware problem | Check the modem's physical connection. Make sure the modem is on and is connected securely to the correct port. Make sure the transmit and receive indicator lights flash when the chat script is running. |

*Table 9-12 Modem Does Not Dial (continued)*

| Problem | Solution |
|---|---|
| No packets of interest defined | • Use the **show running-config** privileged EXEC command to view the router configuration. Check the **dialer-list** command entries to see which access lists, if any, are being used to define interesting traffic.<br>• Make sure that the access lists referenced by the **dialer-list** commands specify all traffic that should bring the link up (interesting traffic).<br>• If necessary, modify the **access list** commands so that they define the proper traffic as interesting. |
| Missing chat script | • Use the **debug chat** privileged EXEC command to check whether there is a chat script running.<br>• If there is no chat script running, use the **start-chat** privileged EXEC command or another appropriate command to start the chat script on the line. |
| Bad chat script | • Establish a reverse Telnet session to the modem, and step through each step of the chat script.<br>• Verify that the command response to each chat script step is correct.<br>• Fix any inconsistencies you find in the chat script. |

## Modem Does Not Answer

When attempting to open a dial-up connection to a modem, the modem does not answer the call.

Table 9-13 describes possilbe causes of and solutions to this problems.

*Table 9-13 Modem Does Not Answer*

| Problem | Solution |
|---|---|
| Incorrect cabling | Check the cabling between the modem and the router. Refer to the *Cisco 805 Router Hardware Installation Guide* for information on how to select the serial cable and how to connect the modem. |
| Modem control not enabled on router | • Observe the remote modem to see whether it is receiving a data terminal ready (DTR) signal from the router. Most modems have a DTR indicator light. Check the modem documentation to interpret the indicator lights.<br>• If the DTR indicator light is on, the modem is seeing a DTR signal from the router. You can also enter the **show line 1** privileged EXEC command to check for DTR. If the Modem state shows the string noDTR, then the router is configured to hold DTR low, and the modem is not seeing a DTR signal.<br>• Configure modem control by entering either the **modem inout** or the **modem ri-is-cd** command in the asynchronous line configuration mode. |
| Remote modem not set to auto-answer | • Check the remote modem to see if it is set to auto-answer. Usually, an AA indicator light will be on when auto-answer is set.<br>• Set the remote modem to auto-answer if it is not already set. To find out how to verify and change the modem's settings, refer to your modem documentation. |
| Wrong telephone line attached to remote modem | • Make sure that you are using the correct telephone line. Replace the remote modem with a telephone, and call again. If the phone rings, you are using the correct telephone line.<br>• Contact the telephone company to make sure that the line is good. |
| Remote modem not attached to a router | • Make sure that the remote modem is attached to a router or other device that is asserting DTR.<br>• Most modems have an LED indicator for DTR. Check to make sure that this indicator comes on. |

## Modem Hangs Up Shortly After Connecting

A dial-up connection is successful but the modem hangs up after 30 to 90 seconds.

Table 9-14 outlines the problems that might cause this symptom and describes solutions to those problems.

*Table 9-14 Modem Hangs Up Shortly After Connecting*

| Problem | Solution |
|---|---|
| Modem speed setting is not locked. | • Enter the **show line 1** privileged EXEC command on the router. The output for the serial port should indicate the currently configured transmit (Tx) and receive (Rx) speeds.<br>• If the line is not configured to the correct speed, use the **speed** command in asynchronous line configuration mode to set the speed on the router line. Set the value to the highest speed in common between the modem and the router port. If for some reason you cannot use flow control, limit the line speed to 9600 bps. Faster speeds are likely to result in lost data.<br>• Use the **show line 1** command again, and confirm that the line speed is set to the desired value.<br>• When you are certain that the router line is configured for the desired speed, initiate a reverse Telnet session to the modem on that line.<br>• Use a modem command string that includes the lock DTE speed command for your modem. See your modem documentation for exact configuration command syntax.<br>The lock DTE speed command, which might also be referred to as *port rate adjust* or *buffered mode*, is often related to the way in which the modem handles error correction. This command varies widely between modems.<br>Locking the modem speed ensures that the modem always communicates with the Cisco router at the speed configured on the Cisco serial port. If this command is not used, the modem will revert to the speed of the data link (the telephone line) instead of communicating at the speed configured on the router. |

*Table 9-14 Modem Hangs Up Shortly After Connecting (continued)*

| Problem | Solution |
|---|---|
| Modem control is not enabled on the router. | • Use the **show line 1** privileged EXEC command on the router. The output for the port should show `inout` or `RIisCD` in the Modem column, which indicates that modem control is enabled on the line of the router.<br>• If necessary, configure modem control by using the **modem inout** command in asynchronous line configuration mode. |
| PPP authentication fails. | • Use the **debug ppp chap** privileged EXEC command to see whether PPP authentication was successful. Check the output for the phrase `Passed authentication with remote`. If you see this output, authentication was successful.<br>• If PPP authentication was not successful, verify the username and password configured on the router. The username and password you enter must be identical to those configured on the router. Usernames and passwords are case-sensitive. |
| Local router not waiting long enough to connect. | • Enter the **show dialer** privileged EXEC command to see the configured dialer timeout. A timeout value of less than 120 seconds will not be long enough.<br>• Configure the local router to wait longer for the connection by entering the **dialer wait-for-carrier-time** command in the serial interface configuration mode. Make sure that you specify at least a 120-second timeout. |
| Chat script problem. | • Enter the **debug chat** privileged EXEC command. If you see the output “Success” at the end of the chat script, the chat script completed successfully.<br>• Make the timeout in the chat script longer at the point where it fails.<br>• If the problem persists, verify that the command response to each chat script step is correct. Open a reverse Telnet session to the modem and step through the chat script.<br>• Fix any inconsistencies you find in the chat script. |

## Dial-Up Client Receives No EXEC Prompt

A remote dial-up client opens a session and appears to be connected, but the user does not receive an EXEC prompt (for example, a `Username>` or `Router>` prompt).

Table 9-15 outlines the problems that might cause this symptom and describes solutions to those problems.

*Table 9-15 Dial-Up Client Receives No EXEC Prompt*

| Problem | Solution |
|---|---|
| Autoselect is enabled on the line | Try to access privileged EXEC mode by entering a carriage return. |
| Line is configured with the **no exec** command. | • Use the **show line 1** privileged EXEC command to view the status of the appropriate line. Check the Capabilities field for the phrase says `EXEC suppressed`. If this is the case, the **no exec** line configuration command is enabled.<br>• Configure the **exec** command in asynchronous line configuration mode to allow EXEC sessions to be initiated. |
| Flow control is not enabled, is enabled only on one device (either DTE or DCE), or is misconfigured. | • Enter the **show line 0** privileged EXEC command, and look for the following in the Capabilities field:<br>`Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out...`<br>If there is no mention of hardware flow control in this field, hardware flow control is not enabled on the line.<br>• Configure hardware flow control on the line using the **flowcontrol hardware** command in asynchronous line configuration mode. If for some reason you cannot use flow control, limit the line speed to 9600 bps. Faster speeds are likely to result in lost data.<br>• After enabling hardware flow control on the router line, initiate a reverse Telnet session to the modem via that line.<br>• Use a modem command string that includes the RTS/CTS flow command for your modem. This command ensures that the modem is using the same method of flow control (that is, hardware flow control) as the Cisco router. See your modem documentation for the exact configuration command syntax. |

*Table 9-15 Dial-Up Client Receives No EXEC Prompt (continued)*

| Problem | Solution |
|---|---|
| Modem speed setting is not locked. | • Enter the **show line 1** privileged EXEC command on the router. The output for the serial port should indicate the currently configured transmit (Tx) and receive (Rx) speeds.<br>• If the line is not configured to the correct speed, use the **speed** command in asynchronous line configuration mode to set the speed on the router line. Set the value to the highest speed in common between the modem and the router port. If for some reason you cannot use flow control, limit the line speed to 9600 bps. Faster speeds are likely to result in lost data.<br>• Use the **show line 1** command again, and confirm that the line speed is set to the desired value.<br>• When you are certain that the router line is configured for the desired speed, initiate a reverse Telnet session to the modem on that line.<br>• Use a modem command string that includes the **lock DTE speed** command for your modem. See your modem documentation for the exact configuration command syntax.<br>The **lock DTE speed** command, which might also be referred to as *port rate adjust* or *buffered mode*, is often related to the way in which the modem handles error correction. This command varies widely between modems.<br>Locking the modem speed ensures that the modem always communicates with the Cisco router at the speed configured on the Cisco serial port. If this command is not used, the modem will revert to the speed of the data link (the telephone line) instead of communicating at the speed configured on the router. |

## Dial-Up Session Sees Garbage

Attempts to establish remote dial-up sessions over a modem to a Cisco router return garbage and ultimately result in no connection to the remote site. Users might see a `Connection Closed by Foreign Host` message.

Table 9-16 outlines causes of this problem and describes possible solutions.

*Table 9-16 Dial-Up Session Sees Garbage*

| Problem | Solution |
|---|---|
| Modem speed setting is not locked. | • Enter the **show line 1** privileged EXEC command on the router. The output for the serial port should indicate the currently configured transmit (Tx) and receive (Rx) speeds.<br>• If the line is not configured to the correct speed, use the **speed** command in asynchronous line configuration mode to set the speed on the router line. Set the value to the highest speed in common between the modem and the router port. If for some reason you cannot use flow control, limit the line speed to 9600 bps. Faster speeds are likely to result in lost data.<br>• Use the **show line 1** command again, and confirm that the line speed is set to the desired value.<br>• When you are certain that the router line is configured for the desired speed, initiate a reverse Telnet session to the modem on that line.<br>• Use a modem command string that includes the **lock DTE speed** command for your modem. See your modem documentation for the exact configuration command syntax.<br>The **lock DTE speed** command, which might also be referred to as *port rate adjust* or *buffered mode*, is often related to the way in which the modem handles error correction. This command varies widely between modems.<br>Locking the modem speed ensures that the modem always communicates with the Cisco router at the speed configured on the Cisco serial port. If this command is not used, the modem will revert to the speed of the data link (the telephone line) instead of communicating at the speed configured on the router. |

## Dial-Up Session Ends Up in Existing Session

A remote dial-up session ends up in an already existing session initiated by another user. That is, instead of getting a login prompt, a dial-up user sees a session established by another user (which might be a UNIX command prompt, a text editor session, and so forth).

Table 9-17 outlines causes of this problems and describes possible solutions.

*Table 9-17 Dial-Up Session Ends Up in Existing Session*

| Problems | Solutions |
|---|---|
| Incorrect cabling. | Check the cabling between the modem and the router. Refer to the *Cisco 805 Router Hardware Installation Guide* for information on how to select the serial cable and how to connect the modem. |
| Modem control is not enabled on the router. | • Enter the **show line 1** privileged EXEC command on the router. The output for the serial port should show `inout` or `RIisCD` in the Modem column, which indicates that modem control is enabled on the router line.<br>• Configure modem control by entering either the **modem inout** or the **modem ri-is-cd** command in the asynchronous line configuration mode. |
| Modem configured for DCD is always high. | • The modem should be reconfigured to have DCD high only on CD, which is usually configured with the **&C1** modem command string. Check your modem documentation for the exact syntax for your modem.<br>• You might have to configure the router line to which the modem is connected with the **no exec** command in asynchronous line configuration mode. Clear the line with the **clear line** privileged EXEC command, initiate a reverse Telnet session with the modem, and reconfigure the modem so that DCD is high only on CD.<br>• End the Telnet session by entering **disconnect** and reconfigure the router line with the **exec** line configuration command. |

## Modem Cannot Send or Receive Data

After a dial-up connection is established, a modem cannot send or receive data of any kind.

Table 9-18 outlines causes of this problem and describes possible solutions.

*Table 9-18 Modem Cannot Send or Receive Data*

| Problem | Solution |
|---|---|
| Modem speed setting is not locked. | • Enter the **show line 1** privileged EXEC command on the router. The output for the serial port should indicate the currently configured transmit (Tx) and receive (Rx) speeds.<br>• If the line is not configured to the correct speed, use the **speed** command in asynchronous line configuration mode to set the speed on the router line. Set the value to the highest speed in common between the modem and the router port. If for some reason you cannot use flow control, limit the line speed to 9600 bps. Faster speeds are likely to result in lost data.<br>• Use the **show line 1** command again, and confirm that the line speed is set to the desired value.<br>• When you are certain that the router line is configured for the desired speed, initiate a reverse Telnet session to the modem on that line.<br>• Use a modem command string that includes the **lock DTE speed** command for your modem. See your modem documentation for the exact configuration command syntax.<br>The **lock DTE speed** command, which might also be referred to as *port rate adjust* or *buffered mode*, is often related to the way in which the modem handles error correction. This command varies widely between modems.<br>Locking the modem speed ensures that the modem always communicates with the Cisco router at the speed configured on the Cisco serial port. If this command is not used, the modem will revert to the speed of the data link (the telephone line) instead of communicating at the speed configured on the router. |

*Table 9-18 Modem Cannot Send or Receive Data (continued)*

| Problem | Solution |
|---|---|
| Hardware flow control not configured on local or remote modem or router | • Enter the **show line 0** privileged EXEC command, and look for the following in the Capabilities field:<br>`Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out...`<br>If there is no mention of hardware flow control in this field, hardware flow control is not enabled on the line.<br>• Configure hardware flow control on the line using the **flowcontrol hardware** command in asynchronous line configuration mode. If for some reason you cannot use flow control, limit the line speed to 9600 bps. Faster speeds are likely to result in lost data.<br>• After enabling hardware flow control on the router line, initiate a reverse Telnet session to the modem via that line.<br>• Use a modem command string that includes the RTS/CTS flow command for your modem. This command ensures that the modem is using the same method of flow control (that is, hardware flow control) as the Cisco router is using. See your modem documentation for the exact configuration command syntax. |
| Problem with dialing modem | Make sure that the dialing modem is operational and is securely connected to the correct port. Check whether another modem works when connected to the same port. |

## Modem Cannot Send or Receive IP Data

After a dial-up connection is established, a modem cannot send or receive IP data.

Table 9-19 outlines causes of this problem and describes possible solutions.

*Table 9-19 Modem Cannot Send or Receive IP Data*

| Problem | Solution |
|---|---|
| IP routing not enabled on local or remote router | Make sure that IP routing is enabled on the local and remote routers. |
| No default gateway specified on PC | • Enter the **show slip** privileged EXEC command. Make sure that the specified IP address is the same as the default gateway specification on the PC.<br>• Check the specified default gateway address on the PC. If the IP address is not correct, specify the correct address. For instructions on verifying and changing the default gateway address on the workstation, refer to the vendor documentation. |
| Hardware flow control not configured on local or remote modem or router | • Enter the **show line 0** privileged EXEC command, and look for the following in the Capabilities field:<br>`Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out...`<br>If there is no mention of hardware flow control in this field, hardware flow control is not enabled on the line.<br>• Configure hardware flow control on the line using the **flowcontrol hardware** command in asynchronous line configuration mode. If for some reason you cannot use flow control, limit the line speed to 9600 bps. Faster speeds are likely to result in lost data.<br>• After enabling hardware flow control on the router line, initiate a reverse Telnet session to the modem via that line.<br>• Use a modem command string that includes the **RTS/CTS** flow command for your modem. This command ensures that the modem is using the same method of flow control (that is, hardware flow control) as the Cisco router is using. See your modem documentation for the exact configuration command syntax. |

*Table 9-19 Modem Cannot Send or Receive IP Data (continued)*

| Problem | Solution |
|---|---|
| Static routes not configured | • Use the **show ip route** privileged EXEC command to check whether there is a static route to the remote network in the routing table.<br>• If there is no static route to the remote network, configure one, using the **ip route** command. The static route should point to the remote network. |
| Domain Name System (DNS) server not specified on router or workstation | • Check whether the workstation and router both have DNS information specified. On the router, use the **show running-config** privileged EXEC command to see if DNS is configured. For information on verifying the workstation configuration, refer to the vendor documentation.<br>• If the router and workstation are not configured to use DNS, use the **ip domain-lookup**, **ip domain-name**, and **ip name-server** commands to configure the router.<br>• Configure a DNS server address in the TCP/IP software on the PC. For more information, refer to the vendor documentation. |

## Modem Does Not Disconnect Properly

The modem does not disconnect properly. Connections to the modem do not terminate when the **quit** command is entered.

Table 9-20 outlines causes of this problem and describes possible solutions.

*Table 9-20 Modem Does Not Disconnect Properly*

| Problem | Solution |
|---|---|
| Modem is not sensing DTR. | Enter the **hangup DTR modem** command string. This command tells the modem to drop carrier when the DTR signal is no longer being received. For the exact syntax of this command, see the your modem documentation. |

*Table 9-20 Modem Does Not Disconnect Properly (continued)*

| Problem | Solution |
|---|---|
| Modem control is not enabled on the router. | • Use the **show line 1** privileged EXEC command on the router. The output should show `inout` or `RIisCD` in the Modem column, which indicates that modem control is enabled on the line of the router.<br>• If necessary, configure modem control by using the **modem inout** command in asynchronous line configuration mode. |

## Link Deactivates Too Quickly

After a dial-up connection is established, the link deactivates too quickly.

Table 9-21 outlines causes of this problem and describes possible solutions.

*Table 9-21 Link Deactivates Too Soon*

| Problem | Solution |
|---|---|
| Dialer timeout is too short | • Use the **show running-config** privileged EXEC command to view the router configuration. Check the value configured with the **dialer idle-timeout** command.<br>• Increase the timeout value, using the **dialer idle-timeout** *seconds* command. The default is 120 seconds. |
| Dialer lists are too restrictive | • Use the **show running-config** privileged EXEC command to view the router configuration. Check the access lists, if any, referenced by **dialer list** commands.<br>• Make sure that the access lists describe all the traffic that should keep the link active. Reconfigure the access lists to include additional traffic if necessary. |

## Link Does Not Deactivate or Stays Activated Too Long

After a dial-up connection is established, the link activates indefinitely or stays activated too long in an idle state.

Table 9-22 outlines causes of this problem and describes possible solutions.

*Table 9-22 Link Does Not Deactivate or Stays Activated Too Long*

| Problem | Solution |
|---|---|
| Dialer lists not restrictive enough | • Use the **show running-config** privileged EXEC command to view the router configuration. Check the access lists, if any, referenced by **dialer list** commands.<br>• Make sure that the access lists do not describe traffic that should not keep the link active. Reconfigure the access lists if necessary. |
| Modems misconfigured | Make sure that the local and remote modems are properly configured. In particular, both modems should be configured to disconnect on loss of DTR (Hangup DTR). For the exact syntax of this command, see your modem documentation. |

## Poor Dial-Up Connection Performance

After a dial-up connection is established, performance over the link is slow or unreliable, often as a result of a high rate of data loss.

Table 9-23 outlines causes of this problem and describes possible solutions.

*Table 9-23 Poor Dial-Up Connection Performance*

| Problem | Solution |
|---|---|
| Error correction is not configured on the modem. | Make certain the modem is configured for error correction. For the exact syntax of the command, see your modem documentation. |
| Flow control is not enabled, is enabled only on one device (either DTE or DCE), or is misconfigured. | • Enter the **show line 0** privileged EXEC command, and look for the following in the Capabilities field:<br>`Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out...`<br>If there is no mention of hardware flow control in this field, hardware flow control is not enabled on the line.<br>• Configure hardware flow control on the line using the **flowcontrol hardware** command in asynchronous line configuration mode. If for some reason you cannot use flow control, limit the line speed to 9600 bps. Faster speeds are likely to result in lost data.<br>• After enabling hardware flow control on the router line, initiate a reverse Telnet session to the modem via that line.<br>• Use a modem command string that includes the **RTS/CTS** flow command for your modem. This command ensures that the modem is using the same method of flow control (that is, hardware flow control) as the Cisco router. See your modem documentation for the exact configuration command syntax. |
| Congestion or line noise. | • If the network is congested, dial-up connections can freeze for a few seconds. The only solution is to reduce congestion on the network by increasing bandwidth or redesigning the network.<br>• Line noise can also freeze up a dial-up connection. For information on how to account for line noise for your modem, refer to the vendor documentation. |

# Frame Relay Problems

This section describes how to troubleshoot the following Frame Relay symptoms:

- Frame Relay Link Is Down, page 9-45
- Cannot Ping Remote Router, page 9-48
- Cannot Ping End to End, page 9-51

## Frame Relay Link Is Down

Connections over a Frame Relay link fail. Table 9-24 outlines causes of this problem and describes possible solutions.

***Table 9-24 Frame Relay Link Is Down***

| Problem | Solution |
|---|---|
| Cabling, hardware, or carrier problem | Perform these steps on the local and remote routers.<br>• Use the **show interfaces serial 0** command to see if the interface and line protocol are up.<br>• If the interface and line protocol are down, refer to the *Cisco 805 Router Hardware Installation Guide* to confirm that you are using the correct serial cable to connect the CSU/DSU and that you connected the CSU/DSU correctly. Make sure that cables are securely attached.<br>• If the cable is correct, try moving it to a different port. If that port works, then the first port is defective. Replace the router.<br>• If the cable does not work on the second port, replace the cable. If it still does not work, there might be a problem with the DCE. Contact your carrier about the problem. |

*Table 9-24 Frame Relay Link Is Down (continued)*

| Problem | Solution |
|---|---|
| Local management interface (LMI) type mismatch | • Use the **show interfaces serial 0** command to check the state of the interface.<br>• If the output shows the interface is up but the line protocol is down, enter the **show frame-relay lmi** privileged EXEC command to see which LMI type is configured on the Frame Relay interface.<br>• Make sure that the LMI type is the same for all devices in the path from source to destination. Enter the **frame-relay lmi-type** {**ansi** \| **cisco** \| **q933a**} command in serial interface configuration mode to change the LMI type on the router. |
| Keepalives not being sent | • Enter the **show interfaces serial 0** command to find out if keepalives are configured. If you see a line that says "keepalives not set," keepalives are not configured.<br>• Use the **keepalive** *seconds* command in serial interface configuration mode to configure keepalives. The default value for this command is 10 seconds. |
| Encapsulation mismatch | • When connecting Cisco devices with non-Cisco devices, you must use Internet Engineering Task Force (IETF) encapsulation on both devices. Check the encapsulation type on the Cisco device by using the **show frame-relay map** privileged EXEC command.<br>• If the Cisco device is not using IETF encapsulation, use the **encapsulation frame-relay ietf** command in serial interface configuration mode to configure IETF encapsulation on the Cisco Frame Relay interface. For information on viewing or changing the configuration of the non-Cisco device, refer to the vendor documentation. |

*Table 9-24 Frame Relay Link Is Down (continued)*

| Problem | Solution |
|---|---|
| Data-link connection identifier (DLCI) inactive or deleted | - Enter the **show frame-relay pvc** privileged EXEC command to view the status of the interface PVC.<br>- If the output shows that the PVC is inactive or deleted, there is a problem along the path to the remote router. Check the remote router or contact your carrier to check the status of the PVC. |
| DLCI assigned to wrong subinterface | - Use the **show frame-relay pvc** privileged EXEC command to check the assigned DLCIs. Make sure that the correct DLCIs are assigned to the correct subinterface.<br>- If the DLCIs appear to be correct, shut down the main interface by entering the **shutdown** command in serial interface configuration mode, then bring the interface back up entering the **no shutdown** command. |

## Cannot Ping Remote Router

Attempts to ping the remote router across a Frame Relay connection fail. Table 9-25 outlines causes of this problem and describes possible solutions.

*Table 9-25 Cannot Ping Remote Router*

| Problem | Solution |
|---|---|
| Encapsulation mismatch | - When connecting Cisco devices to non-Cisco devices, you must use IETF encapsulation on both devices. Check the encapsulation type on the Cisco device by using the **show frame-relay map** privileged EXEC command.<br>- If the Cisco device is not using IETF encapsulation, use the **encapsulation frame-relay ietf** command in serial interface configuration mode to configure IETF encapsulation on the Cisco Frame Relay interface. For information on viewing or changing the configuration of the non-Cisco device, refer to the vendor documentation. |

*Table 9-25 Cannot Ping Remote Router (continued)*

| Problem | Solution |
|---|---|
| DLCI inactive or deleted | • Enter the **show frame-relay pvc** privileged EXEC command to view the status of the interface PVC.<br>• If the output shows that the PVC is inactive or deleted, there is a problem along the path to the remote router. Check the remote router, or contact your carrier to check the status of the PVC. |
| DLCI assigned to wrong subinterface | • Use the **show frame-relay pvc** privileged EXEC command to check the assigned DLCIs. Make sure that the correct DLCIs are assigned to the correct subinterface.<br>• If the DLCIs appear to be correct, shut down the main interface by entering the **shutdown** command in serial interface configuration mode. Then bring the interface back up by entering the **no shutdown** command. |
| Misconfigured access list | • Enter the **show access-list** privileged EXEC command to see whether there are access lists configured on the router.<br>• If access lists are configured, test connectivity by disabling access lists by entering the **no access-group** command in global configuration mode. Check to see whether connectivity is restored.<br>• If connections work, reenable access lists one at a time, checking connections after enabling each access list.<br>• If enabling an access list blocks connections, make sure that the access list does not deny necessary traffic. Make sure to configure explicit **permit** statements for any traffic you want to pass.<br>• Continue testing access lists until all access lists are restored and connections still work. |

*Table 9-25 Cannot Ping Remote Router (continued)*

| Problem | Solution |
|---|---|
| **frame-relay map** command missing | • Enter the **show frame-relay map** privileged EXEC command to see whether an address map is configured for the DLCI.<br>• If you do not see an address map for the DLCI, enter the **clear frame-relay-inarp** privileged EXEC command. Then enter the **show frame-relay map** command again to see if there is now a map to DLCI.<br>• If there is no map to the DLCI, add a static address map by entering the **frame-relay map** command in serial interface configuration mode.[1] For complete information on configuring Frame Relay address maps, refer to the *Cisco IOS Wide-Area Networking Configuration Guide* publication.<br>• Make sure that the DLCIs and next-hop addresses specified in **frame-relay map** commands are correct. The specified protocol address should be in the same network as your local Frame Relay interface. |
| No **broadcast** keyword in **frame-relay map** statements | • Enter the **show running-config** privileged EXEC command on the local and remote routers to view the router configuration. Check **frame-relay map** command entries to see if the **broadcast** keyword is specified.<br>• If the keyword is not specified, add the **broadcast** keyword to all **frame-relay map** commands. By default, the **broadcast** keyword is added to dynamic maps learned via Inverse ARP. |

[1] You can eliminate the need for static Frame Relay address maps by using Inverse Address Resolution Protocol (ARP) instead. Use the **frame-relay interface-dlci** *dlci* **broadcast** interface configuration command to configure an interface to use Inverse ARP. For more information about the use of this command, refer to the *Cisco IOS Wide-Area Networking Configuration Guide* and *Wide-Area Networking Command Reference*.

## Cannot Ping End to End

Attempts to ping devices on a remote network across a Frame Relay connection fail. Table 9-26 outlines causes of this problem and describes possible solutions.

*Table 9-26 Cannot Ping End to End*

| Problem | Solution |
|---|---|
| Split horizon problem | In a partially meshed Frame Relay environment, you must configure subinterfaces to avoid problems with split horizon. For detailed information on configuring subinterfaces, refer to the *Wide-Area Networking Configuration Guide* and *Wide-Area Networking Command Reference*. |
| No default gateway on workstation | • From a local workstation or server, try to ping the remote workstation or server. Make several attempts to ping the remote device if the first ping is unsuccessful.<br>• If all your attempts fail, check to see whether the local workstation or server can ping the Frame Relay interface of the local router.<br>• If you are unable to ping the Frame Relay interface of the local router, check the local workstation or server to see whether it is configured with a default gateway specification.<br>• If there is no default gateway specified, configure the device with a default gateway. The default gateway should be the address of the LAN interface of the local router. For information on viewing or changing the default gateway of the workstation or server, refer to the vendor documentation. |

# X.25 Problems

This section describes how to troubleshoot the following X.25 symptoms:

- No Connections over X.25 Link
- Excess Serial Errors on X.25 Link

## No Connections over X.25 Link

Connections over an X.25 link fail.

Table 9-27 outlines causes of this problem and describes possible solutions.

*Table 9-27 No Connections over X.25 Link*

| Problem | Solution |
|---|---|
| Incorrect cabling or bad router hardware | • Check all cabling and hardware for damage or wear. Replace cabling or hardware as required. For more information on the Cisco 805 router and serial cables, refer to the *Cisco 805 Router Hardware Installation Guide*.<br>• Enter the **show interfaces serial 0** privileged EXEC command to determine the status of the interface.<br>• If the interface is down, see the "Troubleshooting Serial Line Problems" section on page 9-16. If the interface is up but the line protocol is down, check the Link Access Procedure, Balanced (LAPB) state in the output of the **show interfaces serial 0** command.<br>• If the LAPB state is not CONNECT, use the **debug lapb** privileged EXEC command (or attach a serial analyzer) to look for set asynchronous balance mode requests (SABMs) being sent, and for UA packets being sent in reply to SABMs. If UAs are not being sent, one of the other possible problems described in this table is the likely cause.<br>• If the **show interfaces serial 0** command indicates that the interface and line protocol are up but no connections can be made, there is probably a router or switch misconfiguration. Refer to the other possible problems outlined in this table. |
| Link is down | Enter the **show interfaces serial 0** privileged EXEC command to determine whether the link is down. If the link is down, see the "Troubleshooting Serial Line Problems" section on page 9-16. |

*Table 9-27 No Connections over X.25 Link (continued)*

| Problem | Solution |
|---|---|
| Misconfigured protocol parameters | • Enable the **debug lapb** privileged EXEC command and look for set asynchronous balance mode requests (SABMs) being sent. If no SABMs are being sent, disable the **debug lapb** command and enable the **debug x25 events** privileged EXEC command.<br>• Look for `RESTART` messages (for PVCs) or `CLEAR REQUESTS` with non-zero cause codes (for SVCs).<br>• To interpret X.25 cause and diagnostic codes provided in the **debug x25 events** output, refer to the *Debug Command Reference* document.<br>• Verify that all critical LAPB parameters (modulo, T1, N1, N2, and k) and the critical X.25 parameters (modulo, X.121 addresses, SVC ranges, PVC definitions, and default window and packet sizes) match the parameters required by the X.25 service provider. |
| Misconfigured **x25 map** command | • Use the **show running-config** privileged EXEC command to view the router configuration. Look for **x25 map** command entries under the serial interface.<br>• Make sure that **x25 map** commands specify the correct address mappings.<br>• If dynamic routing is being used in the network, verify that the **broadcast** keyword is included in the **x25 map** command.<br>• Make sure that all router X.25 configuration options match the settings of attached switches. Reconfigure the router or the switch as necessary.<br>• Enable the **debug x25 events** privileged EXEC command and look for `RESTART` messages (for PVCs) or `CLEAR REQUESTS` with non-zero cause codes (for SVCs). To interpret X.25 cause and diagnostic codes provided in the **debug x25 events** output, refer to the *Debug Command Reference* document. |

## Excess Serial Errors on X.25 Link

The output of the **show interfaces serial 0** privileged EXEC command shows rejects (REJs), receiver not ready events (RNRs), protocol frame errors (FRMRs), restarts (RESTARTs), or disconnects (DISCs) in excess of 0.5 percent of information frames (IFRAMEs).

**Note** If any of these fields is increasing and represents more than 0.5 percent of the number of IFRAMEs, there is likely a problem somewhere in the X.25 network. There should always be at least one SABM. However, if there are more than 10, the packet switch probably is not responding.

Table 9-28 outlines causes of this problem and describes possible solutions.

*Table 9-28 No Connections over X.25 Link*

| Problem | Solution |
|---|---|
| Incorrect cabling or bad router hardware | • Check all cabling and hardware for damage or wear. Replace cabling or hardware as required. For more information on the Cisco 805 router and serial cables, refer to the *Cisco 805 Router Hardware Installation Guide*.<br>• Enter the **show interfaces serial 0** privileged EXEC command to determine the status of the interface.<br>• If the interface is down, see the "Troubleshooting Serial Line Problems" section on page 9-16. If the interface is up but the line protocol is down, check the LAPB state in the output of the **show interfaces serial 0** command.<br>• If the LAPB state is not CONNECT, use the **debug lapb** privileged EXEC command (or attach a serial analyzer) to look for SABMs being sent, and for UA packets being sent in reply to SABMs. If UAs are not being sent, one of the other possible problems described in this table is the likely cause.<br>• If the **show interfaces serial 0** command indicates that the interface and line protocol are up but no connections can be made, there is probably a router or switch misconfiguration. Refer to the other possible problems outlined in this table. |

# Software Upgrade Methods

Following are the methods for upgrading software on Cisco 800 series and Cisco SOHO series routers:

- 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 the 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

This section describes how to recover a lost enable or enable secret password. The process of recovering a password consists of the following major steps:

1. Changing the Configuration Register
2. Resetting the Router
3. Resetting the Password and Saving Your Changes (for lost enable secret passwords only)
4. Resetting the Configuration Register Value

**Note** These procedures can be done only when you are connected to the router through the console port. These procedures cannot be performed through a Telnet session.

**Note** See the “Hot Tips” section on Cisco Connection Online (CCO) for additional information on replacing enable secret passwords.

# Changing the Configuration Register

Follow these steps to change a configuration register.

**Step 1** Connect an ASCII terminal or a PC running a terminal emulation program to the CONSOLE port on the rear panel of the router. Refer to the “Connecting the Router to a PC” section in the “Installation” chapter of the *Cisco 827 Routers Hardware Installation Guide*.

**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 :

```
820-uut2#sh ver
Cisco Internetwork Operating System Software
IOS (tm) C827 Software (C827-NSY6-M), Version 12.0
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Mon 22-Nov-99 11:20 by dahsue
Image text-base:0x80013170, data-base:0x8081B748

ROM:System Bootstrap, Version 12.0(19990519:174856)
[jakumar-twister_dev 1055], DEVELOPMENT SOFTWARE

Jay uptime is 48 minutes
System returned to ROM by reload
Running default software

CISCO C827 (MPC855T) processor (revision 0x00) with 19456K/1024K bytes
of memory.
Processor board ID 00000000, with hardware revision 0000
CPU rev number 5
Bridging software.
4 POTS Ports
1 Ethernet/IEEE 802.3 interface(s)
1 ATM network interface(s)
128K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)

Configuration register is 0x100
```

**Step 4** Record the setting of the configuration register. It is usually 0x2100 or 0x100.

**Step 5** Record the break setting:

- Break enabled—bit 8 is set to 0.
- Break disabled (default setting)—bit 8 is set to 1.

**Note** To enable break, enter the **config-register 0x01** command while in privileged EXEC mode.

# Resetting the Router

Follow these steps to reset the router.

**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, refer to 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, skip the following "Resetting the Password and Saving Your Changes" section on page 9-59, and complete the password recovery process by performing the steps in the "Resetting the Configuration Register Value" section on page 9-59.

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 "Resetting the Password and Saving Your Changes" section on page 9-59.

## Resetting the Password and Saving Your Changes

Follow these steps to reset your password and save the changes.

**Step 1** Enter the **configure terminal** command to enter 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 configuration mode:

```
Router(config)# exit
```

**Step 4** Save your configuration changes:

```
Router# copy running-config startup-config
```

## Resetting the Configuration Register Value

After you have recovered or reconfigured a password, reset the configuration register value:

**Step 1** Enter the **configure terminal** command to enter 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.

# Managing the Cisco Router Web Setup Tool

The Cisco Router Web Setup tool is a free software configuration utility, supporting the Cisco 800 series DSL routers, the Cisco 806 and 831 dual Ethernet routers, and the Cisco SOHO series routers. It includes a Web-based GUI that offers the following features:

- Simplified setup
- Advanced configuration
- Router security
- Router monitoring

## Pointers to CRWS Documentation

To find the CRWS Introduction, go to:

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

To see the CRWS User’s Guide, go to:

http://www.cisco.com/univercd/cc/td/doc/clckstrt/crws/ugcrws 30.htm.

To see the CRWS Troubleshooting Guide, go to:

http://www.cisco.com/univercd/cc/td/doc/clckstrt/crws/tgcrws 31.htm.

# Cisco IOS Basic Skills

Understanding how to use Cisco IOS software saves time when you are configuring your router. If you need a refresher, take a few minutes to read this chapter. If you are already familiar with Cisco IOS software, see Chapter 7, "Router Feature Configuration," and Chapter 8, "Advanced Router Configuration."

This chapter describes what you need to know before you begin configuring your Cisco 800 series routers with Cisco IOS software (the software that runs your router).

This chapter contains the following sections:

# Configuring the Router from a PC

You can configure your router from a connected PC. For information on how to connect the PC, refer to the *Cisco 826 Routers Hardware Installation Guide*.

After connecting the PC, you need *terminal emulation* software. The PC uses this software to send commands to your router. Table A-1 lists some common types of this software, which are based on the type of PC you are using.

***Table A-1 Terminal Emulation Software***

| PC Operating System | Software |
|---|---|
| Windows 95, Windows 98, Windows NT, Windows XP | HyperTerm (included with Windows software), ProComm Plus |
| Windows 3.1 | Terminal (included with Windows software) |
| Macintosh | ProComm, VersaTerm (supplied separately) |

You can use the terminal emulation software to change settings for the type of device that is connected to the PC, in this case a router. 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, refer to Appendix B, "ROM Monitor." To change the router flow control setting, use the **flowcontrol** line configuration command.

For information on how to enter global configuration mode so that you can configure your router, see the "Entering Global Configuration Mode" section on page A-8.

# 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, how to access each mode, the prompt you see in that mode, and how to exit to a mode or enter the next 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, refer to the Cisco IOS 12.0 documentation set.

*Table A-2 Command Modes Summary*

| Mode | Access Method | Prompt | Exit/Entrance Method | About this Mode |
|---|---|---|---|---|
| User EXEC | Begin a session with your router. | `Router>` | To exit router session, enter the **logout** command. | Use this mode to:<br>• Change terminal settings.<br>• Perform basic tests.<br>• Display system information. |
| Privileged EXEC | Enter the **enable** command from user EXEC mode. | `Router#` | To exit to user EXEC mode, enter the **disable** command.<br>To enter global configuration mode, enter the **configure** command. | Use this mode to:<br>• Configure your router operating parameters.<br>• Perform the verification steps shown in this guide.<br>• To prevent unauthorized changes to your router configuration, access to this mode should be protected with a password as described in "Enable Secret and Enable Passwords" later in this chapter. |

*Table A-2 Command Modes Summary (continued)*

| Mode | Access Method | Prompt | Exit/Entrance Method | About this Mode |
|---|---|---|---|---|
| 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**.<br>To enter interface configuration mode, enter the **interface** command. | Use this mode to configure parameters that apply to your router as a whole.<br>Also, you can access the following modes, which are described later in this table:<br>• Interface configuration<br>• Router configuration<br>• Line configuration |
| Interface configuration | Enter the **interface** command (with a specific interface, such as **interface ethernet 0**) from global configuration mode. | `Router (config-if)#` | To exit to global configuration mode, enter the **exit** command.<br>To exit to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.<br>To enter subinterface configuration mode, specify a subinterface with 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 | Exit/Entrance Method | About this Mode |
|---|---|---|---|---|
| Router configuration | Enter your router command 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.<br>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 | Specify the **line** command with the desired keyword, for example, **line 0**, from global configuration mode. | `Router (config-line)#` | To exit to global configuration mode, enter the **exit** command.<br>To enter 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 at that command mode, enter a question mark:

```
router> ?
access-enableCreate a temporary access-list entry
access-profileApply user-profile to interface
clearReset functions
...
```

To complete a command, enter a few known characters followed by a question mark (with no space):

```
router> s?
* s=show set show slip systat
```

For a list of command variables, enter the **show** command followed by a space and a question mark:

```
router> show ?
clock   Display the system clock
dialerDialer parameters and statistics
exceptionexception information
...
```

To redisplay a command you previously entered, press the up-arrow key. You can continue to press the up arrow key for more commands.

# Enable Secret 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 password)

You must enter an enable secret password 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:

**Step 1** After your router boots up, answer **no** when the following question displays:

```
Would you like to enter the initial configuration dialog [yes]: no
```

**Step 2** Enter the **enable** command:

```
router> enable
```

**Step 3** If you have configured your router with an enable password, enter it when you are prompted.

The enable password does not show on the screen when you enter it. This example shows how to enter privileged EXEC mode:

```
Password: enable_password
router#
```

Enable mode is indicated by the # in the prompt. You can now make changes to your router configuration.

**Step 4** Enter the **configure terminal** command to enter global configuration mode, indicated by `(config)#` in the prompt:

```
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 you entered, you can enter the keyword **no** before most commands; for example, **no ip routing**.

## Command-Line Error Messages

Table A-2 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.<br>The possible keywords that you can enter with the command are displayed. |
| `% Incomplete command.` | You did not enter all of 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.<br>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 of the commands that are available in this command mode. |

# Saving Configuration Changes

You need to enter the **copy running-config startup-config** command to save your configuration changes to nonvolatile RAM (NVRAM) 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 #
```

# Partition and Squeeze

Partition and squeeze are supported on Cisco 831, Cisco 837, SOHO 91, and SOHO 97 routers. When a Flash memory device is full, you may want to rearrange the files so that the space used by the deleted files can be reclaimed. If you wish to permanently delete files on a Flash memory device, you may use the squeeze operation to remove all the deleted files from the Flash file systems and recover the space that the files occupied. The squeeze operation can take as long as several minutes because it involves erasing and rewriting almost an entire Flash memory space. To enable the squeeze operation, all of the Flash device file systems, including the partitions if any, must be erased before the squeeze command can be used. There are provisions in the **erase** command to disable this squeeze utility.

The partition feature requires at least two banks of Flash memory. The partitioning does not cause an existing file in Flash memory to be split across the partitions. The number of partitions that you can create in a Flash memory device is equal to the number of banks in the device, but the maximum number of partitions is 8.

Enter the **router(config)#partition** *flash-filesystem* command to create the partition. The command separates Flash memory into up to 8 partition. The squeeze command will not delete files saved in partition that is not marked as “deleted.”

Enter the #**squeeze** *flash* command to permanently delete all files marked “delete” on a Flash memory device.

Use the following steps to erase an entire Flash memory system, beginning in global configuration mode.

| | Command | Task |
|---|---|---|
| **Step 1** | router(config)# **no partition** *flash-filesystem* | Remove all partitions on the specific Flash file system. The reason for removing partitions is to ensure that the entire Flash file system is erased. The **squeeze** command can be used in a Flash file memory with partitions after the Flash file memory has been erased. |
| **Step 2** | router# **erase** *filesystem* | Erase all of the files on the specified Flash system. |

**Note** The squeeze function is applicable only to the Cisco 831, Cisco 837, Cisco SOHO 91, and Cisco SOHO 97 routers.

# Summary

Now that you have reviewed some Cisco IOS software basics, you can begin to configure your router. Remember the following:

- 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.
- If you want 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, see Chapter 7, “Router Feature Configuration,” and Chapter 8, “Advanced Router Configuration.”

# ROM Monitor

This appendix describes the Cisco 820 series routers ROM monitor (also called the bootstrap program). 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

To use the ROM monitor, you must be using a terminal or PC that is connected to the router over the console port. Refer to the installation chapter in the *Cisco 827 Routers Hardware Installation Guide* that came with the router to connect the router to a PC or terminal.

Perform these steps to configure the router to boot up in ROM monitor mode the next time it is rebooted.

| | Command | Task |
|---|---|---|
| **Step 1** | **enable** | If an enable password is configured, enter the enable command and the enable password to enter privileged EXEC mode. |
| **Step 2** | **configure terminal** | Enter global configuration mode. |
| **Step 3** | **config-reg 0x0** | Reset the configuration register. |
| **Step 4** | **exit** | Exit global configuration mode. |
| **Step 5** | **reload** | Reboot the router with the new configuration register value. The router remains in ROM monitor and does not boot the Cisco IOS software.<br>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 on page B-6.<br>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.

# Who Should Upgrade ROMMON and Why

To ensure proper functionality and prevent router inoperability, upgrade the ROM monitor (ROMMON) image to the latest version before downloading the Cisco IOS image. The ROMMON images are backward compatible with all previously released Cisco IOS software images.

# Where to Find New Versions of ROMMON

Go to the following website for a new versions of ROMMON. You will need to enter your Cisco login account to access the website.

http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml

# Performing the Upgrade

Follow the steps below to upgrade the ROMMON image, beginning in ROMMON mode.

**Step 1** Download the ROMMON image from CCO, and place it on your TFTP server.

**Step 2** Connect the Ethernet cable to the same hub that the TFTP server is attached to.

**Step 3** Place your Cisco router in ROMMON mode by sending the Telnet command break during a router reboot sequence. Make sure that all the parameters are exact and are in capital letters. The following prompt is displayed when the router is in ROMMON mode:

```
rommon 1 >
```

**Step 4** Set the following parameters.

```
rommon 1 > IP_ADDRESS=ip_address
rommon 1 > IP_SUBNET_MASK=ip_subnet_mask
rommon 1 > DEFAULT_GATEWAY=default_gateway
rommon 1 > TFTP_SERVER=TFTP_server
rommon 1 > TFTP_FILE=TFTP_file
rommon 1 >
```

The parameters have the following meanings.

| Parameter | Value |
|---|---|
| IP_ADDRESS= | IP address of the router |
| IP_SUBNET_MASK= | Router subnet mask |
| DEFAULT_GATEWAY= | IP address of the router default gateway |
| TFTP_SERVER= | IP address of the TFTP server on which the ROMMON image is located |
| TFTP_FILE= | The path and file name of the ROMMON image |

**Step 5** Verify parameter settings, using the **set** command. Correct any errors by reentering the parameters and their values. For example:

```
rommon > set

TFTP_CHECKSUM=0
IP_SUBNET_MASK=255.255.255.0
DEFAULT_GATEWAY=1.6.0.1
TFTP_SERVER=223.255.254.254
IP_ADDRESS=1.6.97.20
TFTP_FILE=/auto/tftpload/ROMMON/C820_RM_ALT.srec.122-1r.XE2
```

**Step 6** Upgrade the ROMMON image, using the **tftpdnld -u** command.

**Note** You might be prompted to reset the router in ROMMON mode by entering the **reset** command. If you receive this prompt, reset the router before you perform Step 1 througth Step 5 again.

```
rommon >tftpdnld -u

IP_ADDRESS:1.6.97.20
IP_SUBNET_MASK:255.255.255.0
DEFAULT_GATEWAY:1.6.0.1
TFTP_SERVER:223.255.254.254
TFTP_FILE:/auto/tftpload/ROMMON/C820_RM_ALT.srec.122-1r.XE2
WARNING: alternate copy of rommon exists, filename:C820_RM_ALT.srec
all existing data in the alternate copy of rommon will be lost.
Do you wish to continue? y/n: [n]:
```

**Step 7** Enter **y** to start the download. Successive exclamation points (!!!!!!) indicate that the download is occurring. The router reboots when the download is complete.

## Updating in Cisco IOS EXEC Mode

**Step 1** Download the ROMMON image from CCO, and place it on your TFTP server.

**Step 2** In EXEC mode, save the current configuration, using the **copy running-config startup-config** command.

**Step 3** Enter the **copy tftp rommon** command, and answer the prompts. Replace the variables shown in the following example with the correct values for your router:

```
820-2#copy tftp:rommon:
Address or name of remote host []? IP_address_of_remote_host
Source filename []? rommon_image_source_file_name
Destination filename [rommon]? rommon_image_destination_file_name
```

# 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
dev                  list the device table
dir                  list files in file system
dis                  display instruction stream
dnld                 serial download a program module
frame                print out a selected stack frame
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
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
```

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, refer to the documentation for that product for information on how to send a Break command.

# Command Descriptions

Table B-1 describes the most commonly used ROM monitor commands.

*Table B-1 Most 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:<br>`rommon 16 > dis -?`<br>`usage : dis [addr] [length]`<br>The output for this command is slightly different for the **xmodem** download command:<br>`rommon 11 > xmodem -?`<br>`xmodem: illegal option -- ?`<br>`usage: xmodem [-cyrxu] <destination filename>`<br>`-c  CRC-16`<br>`-y  ymodem-batch protocol`<br>`-r  copy image to dram for launch`<br>`-x  do not launch on download completion`<br>`-u  upgrade ROMMON, System will reboot after upgrade` |

*Table B-1 Most Commonly Used ROM Monitor Commands (continued)*

| Command | Description |
|---|---|
| **reset** or **i** | Resets and initializes the router, similar to a power up. |
| **dev** | Lists boot device identifications on the router; for example:<br>`rommon 10> dev`<br>`Devices in device table:`<br>`        id  name`<br>`    flash:  flash` |
| **dir** *device***:** | Lists the files on the named device; flash, for example:<br>`rommon 4 > dir flash:`<br>`      File size           Checksum   File name`<br>`2835276 bytes (0x2b434c)   0x2073    c806-oy6-mz` |
| boot commands | For more information about the ROM monitor boot commands, refer to the *Cisco IOS Configuration Guide* and the *Cisco IOS Command Reference.* |
| **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. |

# Disaster Recovery with TFTP Download

The standard way to load new software on your router is using the **copy tftp flash** privileged EXEC command from the Cisco IOS software command-line interface (CLI). However, if the router is unable to boot the 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.

## tftpdnld 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 using 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* |
| The name of the file that will be downloaded to the router. | **TFTP_FILE=***filename* |

## Optional Variables

The following variables should be set with these commands before using the **tftpdnld** command.

| Variable | Command |
|---|---|
| Configures how the router displays file download progress.<br>**0**—No progress is displayed.<br>**1**—Exclamation points (!!!) are displayed to indicate file download progress. This is the default setting.<br>**2**—Detailed progress is displayed during the file download process; for example:<br>• Initializing interface.<br>• Interface link state up.<br>• ARPing for 1.4.0.1<br>• 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* |
| Amount of time, in seconds, before the download process times out. The default is 7,200 seconds (120 minutes). | **TFTP_TIMEOUT=** *time* |
| Whether or not the router performs a checksum test on the downloaded image:<br>**1**—Checksum test is performed.<br>**0**—No checksum test is performed. | **TFTP_CHECKSUM=***setting* |

# Using the TFTP Download Command Without Writing the Image to Flash Memory

Follow the steps below to do download new file in ROM monitor mode.

**Step 1** Use the appropriate commands to enter all the required variables and any optional variables described earlier in this section.

**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: 1.3.6.7
      IP_SUBNET_MASK: 255.255.0.0
     DEFAULT_GATEWAY: 1.3.0.1
         TFTP_SERVER: 223.255.254.254
           TFTP_FILE: c806-sy-mz
Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash will be lost!
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.

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 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 command **confreg** followed by the new value of the register in hexadecimal, 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 **confreg** 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, a ROM monitor function, to download over the router console port either a software image or a configuration file. Make sure that the Cisco IOS image is in the same PC where you are to perform this function. 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** 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 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. Default is Xmodem protocol. The protocols differ as follows:<br>• Xmodem supports a 128-block transfer size. Ymodem supports a 1024-block transfer size.<br>• 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. Default is to load the image into Flash memory. |
| **x** | Optional. Image is loaded into DRAM without being executed. |
| *destination_ file_name* | The 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 the steps below to run Xmodem:

**Step 1** Move the image file to the local drive where the 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, error messages are displayed on the console only when the data transfer is terminated.

If an error does occur during a data transfer, the transfer is terminated, and an error message is displayed. 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 the 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, cannot 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
```

# Disaster Recovery with Console Download of Cisco IOS Software

You can use console download, a ROM monitor function, to download over the router console port either a software image or a configuration file. Make sure that the Cisco IOS image is in the same PC where you are to perform this function. After downloading, the file is saved either 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** 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 UART. If the PC serial port is not using a 16550 UART, we recommend using a speed of 38,400 or less when downloading a Cisco IOS image over the console port.

## Command Description

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. Default is Xmodem protocol. The protocols differ as follows:<br>• Xmodem supports a 128-block transfer size. Ymodem supports a 1024-block transfer size.<br>• 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. Default is to load the image into Flash memory. |
| **x** | Optional. Image is loaded into DRAM without being executed. |
| *destination_ file_name* | The 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 the steps below to run Xmodem:

1. Move the image file to the local drive where the Xmodem will execute.
2. Enter the **xmodem** command.

# Error Reporting

Because the ROM monitor console download uses the console to perform the data transfer, error messages are displayed on the console only when the data transfer is terminated.

If an error does occur during a data transfer, the transfer is terminated, and an error message is displayed. 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 the 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, cannot proceed.”
```

The following are ROM monitor debugging commands:

- **stack** or **k**—produce 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
RO = 0x00000000 R1 = 0x80005ea8 R2 = oxffffffff 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 nonvolatile random-access memory (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 0x2
```

```
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 C

# Common Port Assignments

Table C-1 lists currently assigned Transmission Control Protocol (TCP) port numbers. To the extent possible, the User Datagram Protocol (UDP) uses the same numbers.

*Table C-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 |

*Table C-1 Currently Assigned TCP and UDP Port Numbers (continued)*

| Port | Keyword | Description |
|---|---|---|
| 37 | TIME | Time |
| 39 | RLP | Resource Location Protocol |
| 42 | NAMESERVER | Host Name 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 |
| 77 | – | Any private RJE service |
| 79 | FINGER | Finger |
| 95 | SUPDUP | SUPDUP Protocol |
| 101 | HOST NAME | NIC host name server |
| 102 | ISO-TSAP | ISO-Transport Service Access Point (TSAP) |
| 103 | X400 | X400 |
| 104 | X400-SND | X400-SND |
| 111 | SUNRPC | SUN 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 |

*Table C-1 Currently Assigned TCP and UDP Port Numbers (continued)*

| Port | Keyword | Description |
|---|---|---|
| 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 rexec (control) |
| 513 | TCP—rlogin<br>UDP—rwho | TCP—UNIX rlogin<br>UDP—UNIX broadcast name service |
| 514 | TCP—rsh<br>UDP—syslog | TCP—UNIX rsh and log |
| 515 | Printer | UNIX line printer remote spooling |
| 520 | RIP | Routing Information Protocol |
| 525 | Timed | Time server |

# Provisioning an ISDN Line

This appendix describes ISDN lines and switches, the features available, and how to order your ISDN line.

The term *provisioning* refers to the features that you can order for the ISDN line.

If you are in North America and do not use an NI1 switch, Cisco strongly recommends familiarizing yourself with provisioning terminology related to other switch types so that communication with your telephone service provider goes more smoothly.

## Before Ordering an ISDN Line

Before you order an ISDN line, you must decide the following:

- Whether to order only data applications or both data and voice applications. A *data application* is one that runs over a B channel of any Cisco 800 series router. A *voice application* is one that runs over the telephone interface of Cisco 803 or Cisco 804 routers.
- Which data and voice application features you want to order.
- Which ISDN switch to use.
- If you use a National ISDN-1 (NI1) switch, which capability package, if any, to use. A *capability package* is a set of standardized ISDN line features that simplify the ISDN line configuration.

# Data and Voice Applications

You must decide whether to order only data applications or both data and voice applications.

- All Cisco 800 series routers support data applications.
- Cisco 803 and Cisco 804 routers also support voice applications.
- Some telephone service providers charge a lower rate for an ISDN line that supports only data applications.

**Note** If you do not need voice capability on your ISDN line, Cisco recommends provisioning your ISDN line for only data applications.

# Data and Voice Application Features

After you decide which applications to order, you must decide the features you want. Table D-1 describes the data application features supported by the ISDN BRI line, and Table D-2 describes the voice application features.

Contact your telephone service provider to find out if any of these features require an additional fee and the amount of the fee.

*Table D-1 ISDN BRI Data Applications*

| Feature | Description |
|---|---|
| Caller ID calling party identification | Identifies the remote system that originated the call. |
| Subaddressing | Provides locally addressed terminals within a specific ISDN access area. |

*Table D-2 ISDN BRI Voice Applications*

| Feature | Description |
|---|---|
| Speech/3.1-kHz audio-bearer capability | Cisco 803 and Cisco 804 routers support voice applications. |
| Multiple subscriber numbers (MSN) | Supports multiple directory numbers on the same ISDN line. Each piece of terminal equipment is assigned its own directory number. |
| Call holding and retrieving | A call in progress can be put on hold and then retrieved. |
| Call waiting | During a voice call, the call-waiting tone is generated when a second voice call is received. |
| Call bumping | When two data calls are in progress and additional call offering (ACO) is provisioned, the router either ignores a voice call or disconnects a data call to accept the voice call. (Also referred to as voice priority.) |
| Call transferring | Transfers an active call to another telephone number. |
| Three-way call conferencing | Adds a third party to an existing call. |
| Call forwarding | Forwards an incoming call to a third party. |
| Caller ID, calling party identification | Identifies the billing number associated with the line that originated the call. |
| Caller ID | Displays telephone number of remote system that originated the call on a device connected to a telephone port. |

The data and voice applications described in this section might be referred to by different names, depending on the telephone service provider. The terms can differ even within a country. Table D-3 lists the names and codes that could be used by telephone service providers outside of North America.

*Table D-3 ISDN Terms Used Outside the North America*

| North America Name | Other Names | Code |
|---|---|---|
| Call hold and retrieve | Call hold | CH HOLD |
| Call waiting | Anklopfen[1] | CW |
| Multiple subscriber numbers | Extended addressing<br>Selection directe a l’arrive | SDA MSN |

[1] Germany only

# ISDN Switch Types

Geographic location determines the switch types that are available. The following sections describe the switch types available in North America and outside of North America.

## North American ISDN Switches

The Cisco 800 series routers support the following switches in North America:

- National ISDN-1 (NI1) switches comply with ISDN standards. Lucent, Northern Telecom (Nortel), and other manufacturers support these standards.

**Note** Switches that comply with the NI1 standard provide the best performance with the call-bumping feature. If you order this feature, Cisco recommends using an NI1 switch.

- Lucent 5ESS custom switches can run in either custom mode or NI1 mode. In custom mode, the switch can operate in either a point-to-point or a multipoint configuration. Point-to-point configuration supports one piece of terminal equipment on the BRI line and does not require service profile identifiers (SPIDs). Multipoint configuration supports multiple pieces of terminal equipment on the same BRI line and requires SPIDs.

**Note** When ordering a Lucent 5ESS ISDN line to support multiple voice calls, provision the line for call appearances 1 and 2.

- Nortel DMS-100 custom switches support a custom mode used with older terminal equipment.

## International Switches

Cisco 800 series routers support most ISDN BRI lines outside North America, which generally use one of the following switch types:

- EURO-ISDN
- 1TR6
- VN3
- TPH
- Nippon Telegraph and Telephone (NTT)

**Note** The Cisco 800 series routers support 1TR6 switches for data applications only. The routers do not support 1TR6 switches for voice applications.

# NI1 Capability Packages and National ISDN Ordering Codes

A *capability package* is a set of standardized BRI line features that simplify the process of configuring an ISDN line that is connected to an NI1 switch. The capability package ordering codes (also referred to as ISDN Ordering Codes (IOCs) described in this section apply to NI1 switches.

**Note** Cisco 803 and Cisco 804 routers require two SPIDs for the telephone ports to operate simultaneously, so that you can have a data and a voice call at the same time. If a line is assigned only one SPID, the analog telephone ports cannot operate simultaneously.

If you are not using an NI1 switch, you must order your ISDN line configured as described in the "Other Switches" section later in this appendix.

If you have any problems with your ISDN NI1 provisioning, contact Cisco ISDN Support Services (U.S. only). To access this service or to obtain more information, call (800) 553-NETS (6387) and select the Customer Service option.

## Capability Package R

Package R provides circuit-switched data on both B channels (no voice capabilities). Data capabilities include calling number identification. Cisco recommends this NI1 capability package for Cisco 801 and Cisco 802 routers.

## Capability Package S

Package S provides alternate voice and circuit-switched data with no additional features. Cisco recommends this NI1 capability package for Cisco 803 and Cisco 804 routers when you want a minimum feature set.

## Capability Package EZ-1 or U

Package EZ-1 provides alternate voice and circuit-switched data with all the features and capabilities of the router enabled. Cisco recommends this NI1 capability package for Cisco 803 and Cisco 804 routers when a full feature set is needed. The features include flexible calling (three-way call conferencing, call transfer, call hold and retrieve), ACO (call waiting), and call forward variable (CFV).

EZ-1, EZ-ISDN 1, and U refer to the same capability package.

# Other Switches

This section contains provisioning summaries for other switches. Each summary is a list of codes used by the telephone service provider when installing and configuring your line. When you order your ISDN line, photocopy the appropriate summary for your ISDN switch type, and attach it to your order form, which will ensure that your ISDN line is ordered correctly.

The term *provisioning* refers to the features that can be ordered and configured on the ISDN BRI line before terminal equipment, such as the router, can use the features.

Cisco recommends using the BRI switch provisions listed in the “Lucent 5ESS Custom Provisioning” and “Nortel DMS-100 Custom Provisioning” sections in this appendix to support voice priority on one BRI B channel.

Table D-4 provides a list of commonly used ISDN terms and their definitions that you might find helpful when deciding how to provision your ISDN line and when ordering your ISDN line.

*Table D-4 ISDN BRI Line Provisioning Terms*

| Term | Definition |
|---|---|
| CSD | Circuit-switched data—Number of B channels that can be simultaneously connected for circuit-switched data calls. |
| CSD CHL | Circuit-switched data channel—B channels used for data calls. |
| CSD LIMIT | Circuit-switched data limit—Number of data calls made simultaneously. |
| CSV | Circuit-switched voice—Number of B channels simultaneously connected for voice calls. |
| CSV ACO | Circuit-switched voice additional call offering—Indicates an additional call when the B channel is being used. |
| CSV CHL | Circuit-switched voice channel—B channels used for voice calls. |
| CSV LIMIT | Circuit-switched voice limit—Number of voice calls made simultaneously. |
| CSV NBLIMIT | Circuit-switched voice notification busy limit—Number of additional voice calls allowed. |
| EKTS | Key system option—Whether or not a key system is being used. (In a key system, multiple telephone numbers are shared across terminals.) |
| MAXB CHL | Maximum B channels—Number of B channels used simultaneously. |
| MTERM | Maximum terminals—Number of terminals active on the BRI line. |
| TERMTYP | Terminal type—Terminal type used on the BRI line. Valid types for NI1 switches are Type A and Type C. |

# Lucent 5ESS Custom Provisioning

Table D-5 lists the provisioning summary for Lucent 5ESS custom switches.

*Table D-5 Lucent 5ESS Custom Switch Provisioning Summary*

| Line Provision | Configuration |
|---|---|
| 2B1Q line code[1] | N/A |
| 2B&D line | N/A |
| B1 | Circuit-switched data or voice/data[2] |
| B2 | Circuit-switched data or voice/data[3] |
| D | Signaling only |
| MTERM | 1 |
| MAXB CHNL | 2 |
| ACT USR | Y |
| CSD | 2 |
| CSD CHL | Any |
| TERMTYP | Type A |
| DISPLAY | Y |
| CA PREF | 1 |
| CA PREF | 1 |
| CA PREF | 1 |

*Table D-5 Lucent 5ESS Custom Switch Provisioning Summary (continued)*

| Line Provision | Configuration |
|---|---|
| Call transfer | Y |
| Three-way call conferencing | Y |

1. Order this line provision when connecting the router to the U interface.
2. If you do not need voice capability, provision B1 for data only.
3. If you do not need voice capability, provision B2 for data only.

**Note** Incoming voice priority is not available with Lucent 5ESS custom switches.

You can order the following additional features with the Lucent 5ESS custom switch:

- Caller ID, calling party identification
- Call forwarding
- Call pickup

# Nortel DMS-100 Custom Provisioning

Table D-6 lists the provisioning summary for DMS-100 custom switches. Some telephone service providers do not support additional call offering U (ACOU). If your service provider does not support ACOU, use the provisioning summary listed in Table D-7.

*Table D-6 Nortel DMS-100 Custom Provisioning Summary (ACOU Supported)*

| Line Provision | Configuration |
|---|---|
| 2B1Q line code | [1] |
| 2B&D line | N/A |
| Version to Functional Signaling | N/A |
| Issue 2 (NI1) | N/A |
| Call transfer | Yes |

Table D-6 Nortel DMS-100 Custom Provisioning Summary (ACOU Supported) (continued)

| Line Provision | Configuration |
|---|---|
| Three-way call conferencing | Yes |
| TEI | Dynamic |
| CS | Yes |
| EKTS | No |
| Set Option | Key 1-ACOU 1<br>Key 2-AFC |

1. Order this line provision when connecting the router to the U interface.

Table D-7 Nortel DMS-100 Provisioning Summary (ACOU Not Supported)

| Line Provision | Configuration |
|---|---|
| 2B1Q line code | [1] |
| 2B&D line | N/A |
| Version to functional signaling | N/A |
| Issue 2 (NI1) | N/A |
| TEI | Dynamic |
| CACH | No |
| CS | Yes |
| Call transfer | Yes |
| Three-way call conferencing | Yes |
| EKTS | Yes |
| Set option | 2 call appearances |

1. Order this line provision when connecting the router to the U interface.

# ISDN Leased-Line Speeds

The Cisco 800 series routers support ISDN leased-line speeds of 64, 128, and 144 kbps.

# Ordering an ISDN Line

To order an ISDN BRI line, you need to contact your telephone service provider (usually the telephone company) and do the following:

**Step 1** Order a single 128-kbps ISDN BRI line for your router.

The ISDN BRI service provides two bearer channels (B channels) and one data channel (D channel). B channel service operates at 64 kbps and carries user data. D-channel service operates at 16 kbps and carries control and signaling information, although it can support user data transmission.

**Step 2** Order the data and voice features that you want.

If you are planning to use an NI1 switch, you can order a capability package described in the "NI1 Capability Packages and National ISDN Ordering Codes" section in this appendix. If you are planning to use a switch other than an NI1 switch, refer to the provisioning summary information described in either the "Lucent 5ESS Custom Switch" and "Nortel DMS-100 Custom Provisioning" sections in this appendix to select features.

**Step 3** If you have Cisco 803 or Cisco 804 routers, order the additional call offering option if desired.

With this feature, the router can handle voice calls while in use.

**Step 4** Obtain and record the following information from your telephone service provider:

**a.** ISDN switch type.

**b.** Service profile identifiers (SPIDs). SPIDs are numbers assigned only by North American telephone service providers. SPIDS identify the ISDN B channels. The SPID format is generally an ISDN telephone number with several numbers added to it, for example, 40855512340101. Depending on the switch type that supports your ISDN BRI line, your ISDN line could be assigned none, one, or two SPIDs.

# Router Software Configuration Requirements

This section lists configuration requirements for Cisco 800 series routers when using specific BRI switch types.

## NI1 Switch

The following table lists the router configuration requirements when using Cisco 800 series routers with a Lucent 5E NI1 switch in a multipoint configuration.

**Note** The NI1 switch does not support a point-to-point configuration.

*Table D-8 NI1 Configuration*

| Parameter | Configuration | Software Command |
|---|---|---|
| Switch type | NI1 | **isdn switch-type basic-ni1**[1] |
| SPID, directory number | Cisco 801 and 802 routers require one SPID;<br>Cisco 803 and 804 routers require two SPIDs. | **isdn spid1** *spid-number ldn*[2]<br>**isdn spid2** *spid-number ldn* |

[1] If the automatic detection of ISDN switch type is enabled, you do not need to enter this command.

[2] If the automatic detection of SPIDs is enabled, you do not need to specify the actual SPID number provided by your telephone service provider; instead, you can specify any number or numerical string, such as 0.

# Lucent 5ESS Custom Switch

This section describes the router configuration requirements for using Cisco 800 series routers with a Lucent 5ESS custom switch.

## Point-to-Point Configuration

Table D-9 lists the router configuration requirements for using a Lucent 5ESS custom switch in a point-to-point configuration.

***Table D-9 Lucent 5ESS Custom Point-to-Point Configuration***

| Parameter | Configuration | Software Command |
|---|---|---|
| Switch type | 5ESS | **isdn switch-type basic-5ess**[1] |
| SPIDs, directory number | SPIDs are not required; directory number is optional | **isdn spid1** *spid-number ldn*[2]<br>**isdn spid2** *spid-number ldn* |

[1] If the automatic detection of ISDN switch type is enabled, you do not need to enter this command.

[2] If SPIDs are not used or if the automatic detection of SPIDs is enabled, you do not need to specify an actual SPID number provided by your telephone service provider; instead, you can specify any number or numerical string, such as 0.

## Multipoint Configuration

Table D-10 lists the router configuration requirements for using Lucent 5ESS custom switch in a multipoint configuration.

*Table D-10 Lucent 5ESS Custom Multipoint Configuration*

| Parameter | Configuration | Software Command |
|---|---|---|
| Switch type | 5ESS | **isdn switch-type basic-5ess**[1] |
| SPIDs, directory number | Cisco 801 and Cisco 802 routers require one SPID; Cisco 803 and Cisco 804 routers require two SPIDs; directory number is recommended | **isdn spid1** *spid-number ldn*[2]<br>**isdn spid2** *spid-number ldn* |

1. If the automatic detection of ISDN switch type is enabled, you do not need to enter this command.
2. If the automatic detection of SPIDs is enabled, you do not need to specify the actual SPID number provided by your telephone service provider; instead, you can specify any number or numerical string, for example, 0.

# Nortel DMS-100 Switch

This section describes the router configuration requirements for using Cisco 800 series routers with a DMS-100 switch.

## Configure a Router Only

Table D-11 lists the router configuration requirements for using the router only on a Nortel DMS-100 line.

*Table D-11 Nortel DMS-100—Router Only*

| Parameter | Configuration | Software Command |
|---|---|---|
| Switch type | DMS | **isdn switch-type basic-dms100**[1] |
| SPIDs, directory numbers | Two required | **isdn spid1** *spid-number ldn*[2]<br>**isdn spid2** *spid-number ldn* |

1. If the automatic detection of ISDN switch type is enabled, you do not need to enter this command.

2. If the automatic detection of SPIDs is enabled, you do not need to specify the actual SPID number provided by your telephone service provider; instead, you can specify any number or numerical string, such as 0.

## Configure a Router and One Device

Table D-12 lists the router configuration requirements for using a Nortel DMS-100 switch when using the router and one device on the ISDN line.

**Note** In this configuration, the router can use only one B channel.

*Table D-12 Nortel DMS-100—Router and One Device*

| Parameter | Configuration | Software Command |
|---|---|---|
| Switch type | DMS | **isdn switch-type basic-dms100**[1] |
| SPIDs, directory number | One required | **isdn spid1** *spid-number ldn*[2]<br>**isdn spid2** *spid-number ldn* |

1. If the automatic detection of ISDN switch type is enabled, you do not need to enter this command.
2. If the automatic detection of SPIDs is enabled, you do not need to specify the actual SPID number provided by your telephone service provider; instead, you can specify any number or numerical string, such as 0.

# Configuration Requirements for Switches Outside North America

ISDN BRI lines used outside North America are not assigned SPIDs. The optional argument, *spid-number*, in some of the software commands should be ignored or omitted if you are connecting to a line that does not use SPIDs.

## 1TR6 Switch

The 1TR6 lines can be configured for multiple subscriber numbers, usually referred to as “extended addressing” in Germany. The line is usually assigned a group of eight sequential directory numbers that can be used for the different pieces of terminal equipment used on the BRI line. These numbers are also used for allocation to the analog telephone port and for call routing.

# ISDN BRI Cause Values

This appendix describes ISDN BRI standard cause values that might be received from the ISDN switch when using Cisco 800 series routers. These values are sent from the ISDN switch to the router to indicate ISDN call status.

Although telephone service providers generally define cause messages with decimal values, Cisco 800 series routers display the hexadecimal (or *hex*) translation of the decimal value.

Cause values are standardized; however, each telephone service provider uses its own version of the cause message wording. Therefore, the cause messages shown in Table E-1 might not match the messages exactly as they appear on the terminal.

Table E-1 lists the ISDN BRI cause values, the hexadecimal translation, the cause message, and a short definition of the cause message.

*Table E-1 ISDN BRI Cause Values and Cause Messages*

| Cause Value[1] | Hex Value[2] | Cause Message | Definition |
|---|---|---|---|
| 1 | 0001 | Unassigned number. | The ISDN number was sent to the switch in the correct format; however, the number is not assigned to any destination equipment. |
| 2 | 0002 | No route to specified transit network. | The ISDN exchange is asked to route the call through an unrecognized intermediate network. |
| 3 | 0003 | No route to destination. | The call was routed through an intermediate network that does not serve the destination address. |

*Table E-1 ISDN BRI Cause Values and Cause Messages (continued)*

| Cause Value[1] | Hex Value[2] | Cause Message | Definition |
|---|---|---|---|
| 6 | 0006 | Channel unacceptable. | The service quality of the specified channel is insufficient to accept the connection. |
| 7 | 0007 | Call awarded and delivered. | The user is assigned an incoming call that is connected to a channel with an established call. |
| 16 | 0010 | Normal call clearing. | Normal call clearing has occurred. |
| 17 | 0011 | User busy. | The called system acknowledges the connection request but is unable to accept the call because all B channels are in use. |
| 18 | 0012 | No user responding. | The connection cannot be completed because the destination does not respond to the call. |
| 19 | 0013 | No answer from user (user alerted). | The destination responds to the connection request but fails to complete the connection within the prescribed time. The problem is at the remote end of the connection. |
| 21 | 0015 | Call rejected. | The destination is capable of accepting the call, but rejected the call for an unknown reason. |
| 22 | 0016 | Number changed. | The ISDN number used to set up the call is not assigned to any system. (If an alternate address is assigned to the called equipment, it might be returned in the diagnostic field of this message.) |
| 26 | 001A | Nonselected user clearing. | The destination is capable of accepting the call but rejected the call because it was not assigned to the user. |

*Table E-1 ISDN BRI Cause Values and Cause Messages (continued)*

| Cause Value[1] | Hex Value[2] | Cause Message | Definition |
|---|---|---|---|
| 27 | 001B | Destination out of order. | The destination cannot be reached because the interface is not functioning correctly, and a signaling message cannot be delivered. This might be a temporary condition but could last for an extended period of time. For example, the remote equipment might be turned off. |
| 28 | 001C | Invalid number format. | The connection could not be established because the destination address was presented in an unrecognizable format or because the destination address was incomplete. |
| 29 | 001D | Facility rejected. | The facility requested by the user cannot be provided by the network. |
| 30 | 001E | Response to STATUS ENQUIRY. | The status message was generated in direct response to the receipt of a status inquiry message. |
| 31 | 001F | Normal, unspecified. | Reports the occurrence of a normal event when no standard cause applies. No action required. |
| 34 | 0022 | No circuit or channel available. | The connection cannot be established because no appropriate channel is available to take the call. |
| 38 | 0026 | Network out of order. | The destination cannot be reached because the network is not functioning correctly, and the condition might last for an extended period of time. An immediate reconnect attempt will probably be unsuccessful. |
| 41 | 0029 | Temporary failure. | An error occurred because the network is not functioning correctly. The problem will be resolved shortly. |

*Table E-1 ISDN BRI Cause Values and Cause Messages (continued)*

| Cause Value[1] | Hex Value[2] | Cause Message | Definition |
|---|---|---|---|
| 42 | 002A | Switching equipment congestion. | The destination cannot be reached because the network switching equipment is temporarily overloaded. |
| 43 | 002B | Access information discarded. | The network cannot provide the requested access information. |
| 44 | 002C | Requested circuit or channel not available. | The remote equipment cannot provide the requested channel for an unknown reason. This might be a temporary problem. |
| 47 | 002F | Resource unavailable, unspecified. | The requested channel or service is unavailable for an unknown reason. This might be a temporary problem. |
| 49 | 0031 | Quality of service unavailable. | The requested quality of service (as defined by CCITT[3] recommendation X.213) cannot be provided by the network. This might be a subscription problem. |
| 50 | 0032 | Requested facility not subscribed. | The remote equipment supports the requested supplementary service, but only by subscription. |
| 57 | 0039 | Bearer capability not authorized. | The user requested a bearer capability (BC) that the network provides, but that the user is not authorized to use. This might be a subscription problem. |
| 58 | 003A | Bearer capability not presently available. | The network normally provides the requested BC but not at the present time. This might be due to a temporary network problem or to a subscription problem. |
| 63 | 003F | Service or option not available, unspecified. | The network or remote equipment was unable to provide the requested service option for an unspecified reason. This might be a subscription problem. |

*Table E-1 ISDN BRI Cause Values and Cause Messages (continued)*

| Cause Value[1] | Hex Value[2] | Cause Message | Definition |
|---|---|---|---|
| 65 | 0041 | Bearer capability not implemented. | The network cannot provide the bearer capability (BC) requested by the user. |
| 66 | 0042 | Channel type not implemented. | The network or the destination equipment does not support the requested channel type. |
| 69 | 0045 | Requested facility not implemented. | The remote equipment does not support the requested supplementary service. |
| 70 | 0046 | Only restricted digital information bearer is available. | The network is unable to provide unrestricted digital information BC. |
| 79 | 004F | Service or option not available, unspecified. | The network or remote equipment is unable to provide the requested service option for an unspecified reason. This might be a subscription problem. |
| 81 | 0051 | Invalid call reference value. | The remote equipment received a call with a call reference that is not currently in use on the user-network interface. |
| 82 | 0052 | Identified channel does not exist. | The receiving equipment is requested to use a channel that is not activated on the interface for calls. |
| 83 | 0053 | A suspended call exists but this call identity does not. | The network received a call resume request. The call resume request contained a Call Identify information element that indicates that the call identity is being used for a suspended call. |
| 84 | 0054 | Call identity in use. | The network received a call resume request. The call resume request contained a Call Identify information element that indicates that it is in use for a suspended call. |

Table E-1 ISDN BRI Cause Values and Cause Messages (continued)

| Cause Value[1] | Hex Value[2] | Cause Message | Definition |
|---|---|---|---|
| 85 | 0055 | No call suspended. | The network received a call resume request when there was not a suspended call pending. This might be a transient error that will be resolved by successive call retries. |
| 86 | 0056 | Call having requested call identity has been cleared. | The network received a call resume request. The call resume request contained a Call Identity information element, which once indicated a suspended call. However, the suspended call was cleared either by timeout or by the remote user. |
| 88 | 0058 | Incompatible destination. | Indicates that an attempt was made to connect to non-ISDN equipment, such as an analog line. |
| 91 | 005B | Invalid transit network specified. | The ISDN exchange was asked to route the call through an unrecognized intermediate network. |
| 95 | 005F | Invalid message, unspecified. | An invalid message was received, and no standard cause applies. This is usually due to a D-channel error. If this error occurs systematically, report it to your telephone service provider. |
| 96 | 0060 | Mandatory information element is missing. | The receiving equipment received a message that did not include one of the mandatory information elements. This is usually due to a D-channel error. If this error occurs systematically, report it to your telephone service provider. |

*Table E-1 ISDN BRI Cause Values and Cause Messages (continued)*

| Cause Value[1] | Hex Value[2] | Cause Message | Definition |
|---|---|---|---|
| 97 | 0061 | Message type nonexistent or not implemented. | The receiving equipment received an unrecognized message, either because the message type was invalid or because the message type was valid but not supported. Cause 97 is due to either a problem with the remote configuration or a problem with the local D channel. |
| 98 | 0062 | Message incompatible with call state or message type nonexistent. | The remote equipment received an invalid message, and no standard cause applies. Cause 98 is due to a D-channel error. If this error occurs systematically, report it to your telephone service provider. |
| 99 | 0063 | Information element nonexistent or not implemented. | The remote equipment received a message that includes information elements, which were not recognized. This is usually due to a D-channel error. If this error occurs systematically, report it to your telephone service provider. |
| 100 | 0064 | Invalid information element contents. | The remote equipment received a message that includes invalid information in the information element. This is usually due to a D-channel error. |
| 101 | 0065 | Message not compatible with call state. | The remote equipment received an unexpected message that does not correspond to the current state of the connection. This is usually due to a D-channel error. |
| 102 | 0066 | Recovery on timer expiry. | An error-handling (recovery) procedure was initiated by a timer expiration. This is usually a temporary problem. |
| 111 | 006F | Protocol error, unspecified. | An unspecified D-channel error when no other standard cause applies. |

*Table E-1 ISDN BRI Cause Values and Cause Messages (continued)*

| Cause Value[1] | Hex Value[2] | Cause Message | Definition |
|---|---|---|---|
| 127 | 007F | Interworking, unspecified. | An event occurred, but the network does not provide causes for the action that it takes. The precise problem is unknown. |
| UNKNOWN | N/A | Unknown or local error. | An event occurred, but the network does not provide causes for the action that it takes. The precise problem is unknown. |

[1] Cause value is shown in decimal format.

[2] Hex value = hexadecimal translation of the decimal cause value.

[3] CCITT = Consultative Committee for International Telegraph and Telephone.

# INDEX