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 826, 827, 828, 831, 836, and 837 and Cisco SOHO 76, 77, 78, 91, 96, and 97 Routers Software Configuration Guide

Part Number: 78-14565-03 S/W Release (if applicable):

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

ATTN DOCUMENT RESOURCE CONNECTION
CISCO SYSTEMS INC
170 WEST TASMAN DRIVE
SAN JOSE CA 95134-9883

Cisco 826, 827, 828, 831, 836, and 837 and Cisco SOHO 76, 77, 78, 91, 96, and 97 Routers 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-7814565=
Text Part Number: 78-14565-03

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Breakthrough, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0301R)

Cisco 826, 827, 828, 831, 836, and 837 and Cisco SOHO 76, 77, 78, 91, 96, and 97 Routers Software Configuration Guide

CONTENTS

APPENDIX A

APPENDIX B

APPENDIX C

About This Guide

This preface discusses the audience, organization, 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.

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

- Cisco 826 router and Cisco SOHO 76 router
- Cisco 827 router and Cisco SOHO 77 router
- Cisco 828 router and Cisco SOHO 78 router
- Cisco 831 router and Cisco SOHO 91 router
- Cisco 836 router and Cisco SOHO 96 router
- Cisco 837 router and Cisco SOHO 97 router

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.

Refer to the "Organization" section of this preface to help you decide which chapter(s) contains the information you need to configure your software.

Organization

This guide contains the following information:

- Chapter 1, "Concepts"—Provides general concept explanations of features.
- Chapter 2, "Network Scenarios"—Describes five Internet access scenarios and one voice scenario, each featuring the Cisco 827 router, with their specific network topologies and configurations.
- Chapter 3, "Basic Router Configuration"—Explains basic router configuration, feature by feature.
- Chapter 4, "Advanced Router Configuration"—Explains advanced router configuration features.
- Chapter 5, "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.

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 this product:

- Cisco 826 and Cisco SOHO 76 routers:
  - *Cisco 826 and Cisco SOHO 76 Routers Hardware Installation Guide*—Provides detailed instructions for installing Cisco 826 and Cisco SOHO 76 routers.
  - *Cisco 826 and Cisco SOHO 76 Router Cabling and Setup Quick Start Guide*—Provides instructions for quickly cabling and powering up Cisco 828 and SOHO 78 routers.
- Cisco 827 and Cisco SOHO 77 routers:
  - *Cisco 827 Routers Hardware Installation Guide*—Provides detailed instructions for installing the Cisco 827 and Cisco SOHO 77 routers.
  - *Quick Start Guide - Installing Your Cisco 827 Routers*—Provides instructions for quickly cabling and powering up Cisco 827 and Cisco SOHO 77 routers.
- Cisco 828 and SOHO 78 routers:
  - *Cisco 828 Router and SOHO 78 Router Hardware Installation Guide*—Provides detailed instructions for installing the Cisco 828 and SOHO 78 routers.
- Cisco 831 and SOHO 91 routers:
  - *Cisco 831 Router and SOHO 91 Router Hardware Installation Guide*—Provides detailed instructions for installing the Cisco 831 and Cisco SOHO 91 routers.
  - *Cisco 831 Router and SOHO 91 Router Cabling and Setup Quick Start Guide*—Provides detailed instructions on quickly cabling and powering up Cisco 831 and 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 SOHO 97 routers:
  - *Cisco 837 Router and SOHO 97 Router Hardware Installation Guide*—Provides detailed instructions for installing the Cisco 837 and Cisco SOHO 97 routers.
  - *Cisco 837 Router and SOHO 97 Router Cabling and Setup Quick Start Guide*—Provides detailed instructions on quickly cabling and powering up Cisco 837 and 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.

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 or Network Administrators when configuring Cisco routers. To review some typical network scenarios, refer to "Network Scenarios" in Chapter 2. For information on specific configurations, refer to Chapter 3, "Basic Router Configuration" and Chapter 4, "Advanced Router Configuration."

The following topics are included in this chapter:

Overview

The Cisco 826, 827, 828, 831, 836, and 837 and Cisco SOHO 76, 77, 78, 91, 96, and 97 routers are Cisco IOS-based members of the Cisco 800 router family with ATM/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, SOHO 76, and SOHO 77 have one 10Base-T Ethernet and one ADSL-over-ISDN or ADSL network port, respectively.

The data and voice Cisco 827-4V has four FXS/POTS ports in addition to the 10Base-T Ethernet 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 asymmetric digital subscriber line (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 a Cisco IOS-based member of the Cisco 800 router family with ATM/SHDSL support. The 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 SOHO 78 router provide a 4-port Ethernet hub, in addition to the G.SHDSL port.

Both the Cisco 831 router and the 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 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 router and SOHO 97 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 SOHO 97 router offers software encryption capability without hardware encryption.

The Cisco 831, Cisco 836, Cisco 837, SOHO 91, SOHO 96, and SOHO 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 Ethernet	831, 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 surfing, video-on-demand, and remote LAN access.

SHDSL

SHDSL is a technology based on the G.SHDSL (G.991.2) standard that allows both data and voice to be transmitted over the same line. SHDSL is a packet-based network technology that allows high-speed transmission over twisted-pair copper wire between a network service provider (NSP) central office and a customer site, or on local loops created within either a building or a campus.

G.SHDSL devices can extend 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.

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.

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

Routing Protocol Options

Routing protocols include the following:

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

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

Table 1-2 RIP and Enhanced IGRP Comparison

Protocol	Ideal Topology	Metric	Routing Updates
RIP	Suited for topologies with 15 or fewer hops.	Hop count. Maximum hop count is 15. Best route is one with lowest hop count.	By default, every 30 seconds. You can reconfigure this value and also use triggered extensions to RIP.
Enhanced IGRP	Suited for large topologies with 16 or more hops to reach a destination.	Distance information. Based on a successor, which is a neighboring router that has a least-cost path to a destination that is guaranteed to not be part of a routing loop.	Hello packets sent every 5 seconds 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 “Obtaining Documentation” in “About This Guide.”

Enhanced IGRP

Enhanced IGRP is an advanced Cisco proprietary distance-vector and link state routing protocol, which means it uses a metric more sophisticated than distance (hop count) for route selection. Enhanced IGRP uses a metric based on a successor, which is a neighboring router that has a least-cost path to a destination that is guaranteed not to be part of a routing loop. If a successor for a particular destination does not exist but neighbors advertise the destination, the router must recompute a route.

Each router 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 where 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 where 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

Ethernet

Ethernet is a baseband LAN protocol that transports data and voice packets to the WAN interface using carrier sense multiple access collision detect (CSMA/CD). The term is now often used to refer to all CSMA/CD LANs. Ethernet was designed to serve in networks with sporadic, occasionally heavy traffic requirements, 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 adaption 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 the router 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 Routes
- Dialer Watch

Backup Interface

A backup interface is an interface that stays idle until certain circumstances occur, such as WAN downtime, at which point it is activated. The backup interface can be a physical interface such as 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 down when the primary line fails, and the backup interface quickly identifies such failures.

Floating Static Routes

Floating static routes are static routes that have an administrative distance greater than the administrative distance of dynamic routes. Administrative distances can be configured on a static route so that the static route is less desirable than a dynamic route. In this manner, the static route is not used when the dynamic route is available. However, if the dynamic route is lost, the static route can take over, and the traffic can be sent through this 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.

DHCP 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.

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** command and the **session target** command.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 queueing; ATM queues and Cisco IOS queues. CBWFQ is applied to Cisco IOS queues. A first-in-first-out (fifo) Cisco IOS queue is automatically created when a PVC is created. If you use CBWFQ to create classes and attach them to a PVC, a queue is created for each class.

CBWFQ ensures that queues have sufficient bandwidth and that traffic gets predictable service. Low-volume traffic streams are preferred; high-volume traffic streams share the remaining capacity, obtaining equal or proportional bandwidth.

RSVP

RSVP enables routers to reserve enough bandwidth on an interface to ensure reliability and quality performance. RSVP allows end systems to request a particular QoS from the network. Real-time voice traffic requires network consistency. Without consistent QoS, real-time traffic can experience jitter, insufficient bandwidth, delay variations, or information loss. RSVP works in conjunction with current queuing mechanisms. It is up to the interface queuing mechanism (such as CBWFQ) to implement the reservation.

RSVP works well on PPP, HDLC, and similar serial-line interfaces. It does not work well on multi-access LANs. RSVP can be equated to a dynamic access list for packet flows.

You should configure RSVP to ensure QoS if the following conditions describe your network:

- Small-scale voice network implementation
- Links slower than 2 Mbps
- Links with high utilization
- Need for the best possible voice quality

Low Latency Queuing

Low latency queuing (LLQ) provides a low-latency strict priority transmit queue for real-time traffic. Strict priority queuing allows delay-sensitive data to be dequeued and sent first (before packets in other queues are dequeued), giving delay-sensitive data preferential treatment over other traffic.

Access Lists

With basic standard and static extended access lists, you can approximate session filtering by using the established keyword with the **permit** command. The established keyword filters TCP packets based on whether the ACK or RST bits are set. (Set ACK or RST bits indicate that the packet is not the first in the session and the packet therefore belongs to an established session.) This filter criterion would be part of an access list applied permanently to an interface.

Network Scenarios

This chapter includes some example network scenarios and their configurations using Cisco 827 and Cisco 827-4V routers and Cisco 831, Cisco 836, Cisco 837, Cisco SOHO 91, Cisco SOHO 96, and Cisco SOHO 97 routers. This chapter is useful if you are building a new network and want some guidance. Most of the lessons here can be applied as well to networks incorporating Cisco 826, Cisco 828, Cisco SOHO 76, Cisco SOHO 77, and/or Cisco SOHO 78 routers.

Note To verify that a feature is compatible with your router, you can use the software advisor too.

If you already have a network set up and you want to add specific features, see Chapter 3, "Basic Router Configuration" and Chapter 4, "Advanced Router Configuration."

The following sections are included in this chapter:

- Cisco 827 Router Network Connections, page 2-2
- Cisco 831 Router Virtual Private Network Connections, page 2-3
- Cisco 836 or Cisco SOHO 96 Network Connection, page 2-4
- Cisco 837 Router Network Connections, page 2-5
- Internet Access Scenarios, page 2-6
- Configuring Dial Backup, page 2-16
- Configuring the DHCP Server, page 2-39
- Voice Scenario, page 2-55

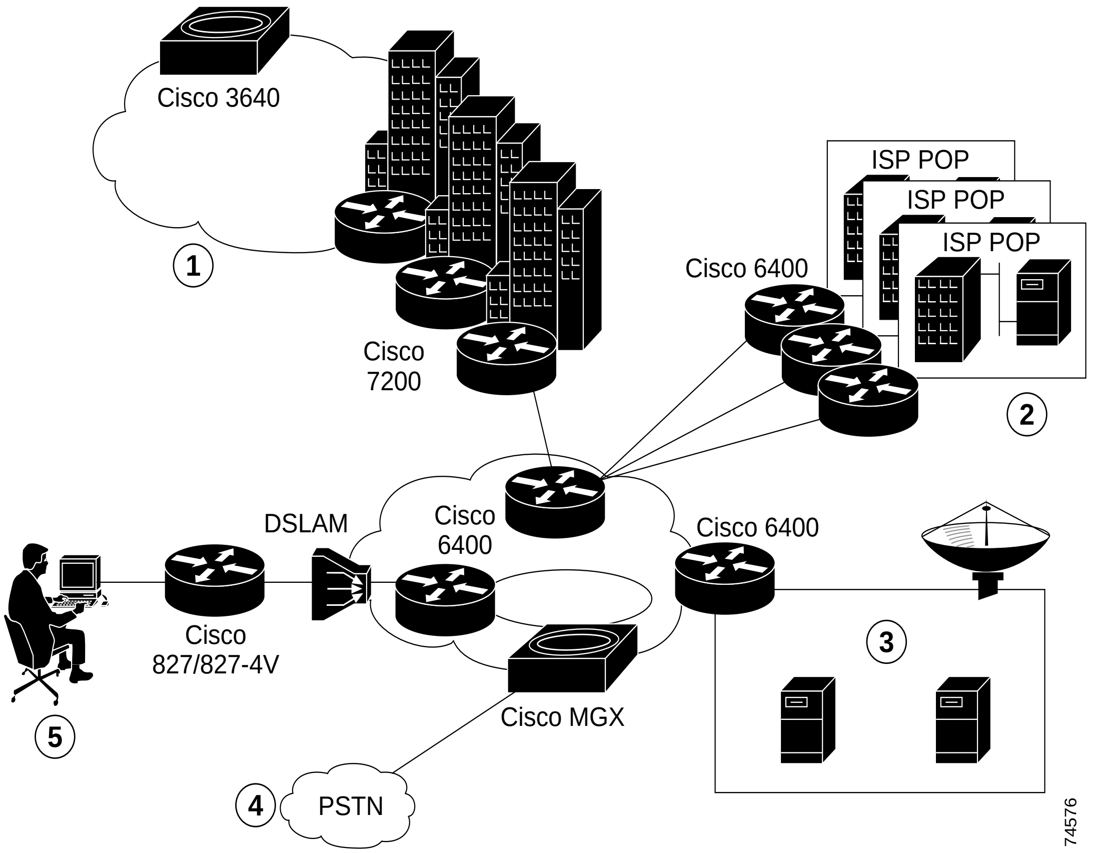
Each scenario in this chapter is described with a network diagram and configuration network examples are provided as models after which you can pattern your network. They cannot, however, anticipate all of your network needs. You can choose not to use features presented in the examples or to add or substitute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

Cisco 827 Router Network Connections

Figure 2-1 illustrates an example network topology employing Cisco 827 routers connecting to the following:

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

Figure 2-1 Cisco 827 Routers Network Connections



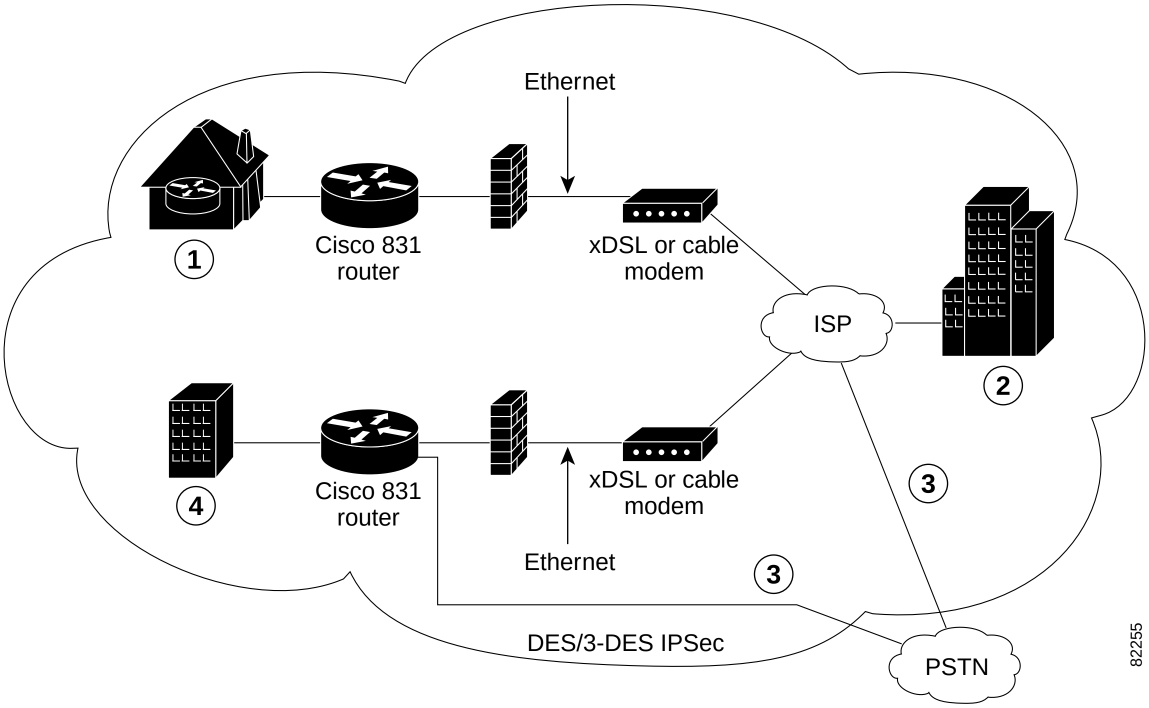
1	Corporate network connecting through a Cisco 3640 voice gateway	**4**	Data and voice local exchange carrier connecting through a Cisco MGX voice gateway
2	Wholesale ISP business	**5**	Small business or remote user, connecting to the network through a Cisco 827/827-4V router
3	ISP POP (data center)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

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

Cisco 831 Router Virtual Private Network Connections

Figure 2-2 shows how a Cisco 831 router can be used in a Virtual Private Network (VPN). The 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 2-2 Cisco 831 Router Virtual Private Network



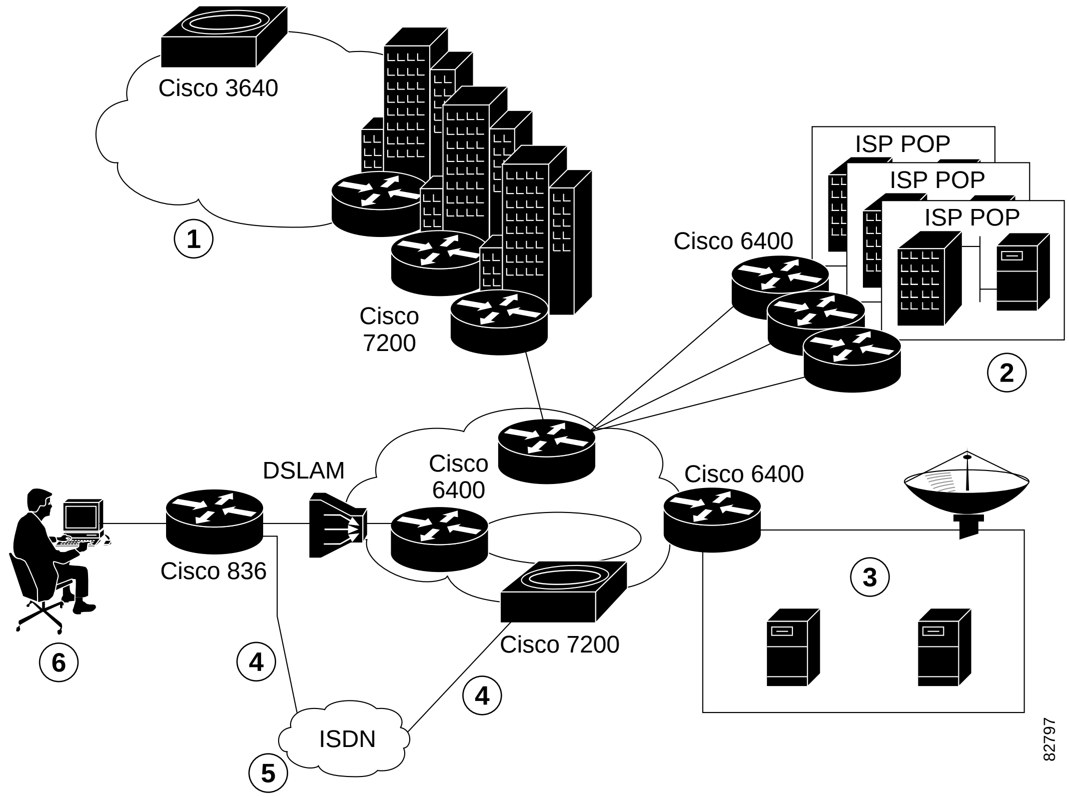
1	Small business or remote user, connecting to the network through a Cisco 831 router.	**3**	Dial backup, as a failover link when primary line goes down
2	Corporate network connecting through a Cisco router	**4**	Branch office network connecting through a Cisco router

Cisco 836 or Cisco SOHO 96 Network Connection

Figure 2-3 shows 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 2-3 Cisco 836 Router Network Connections



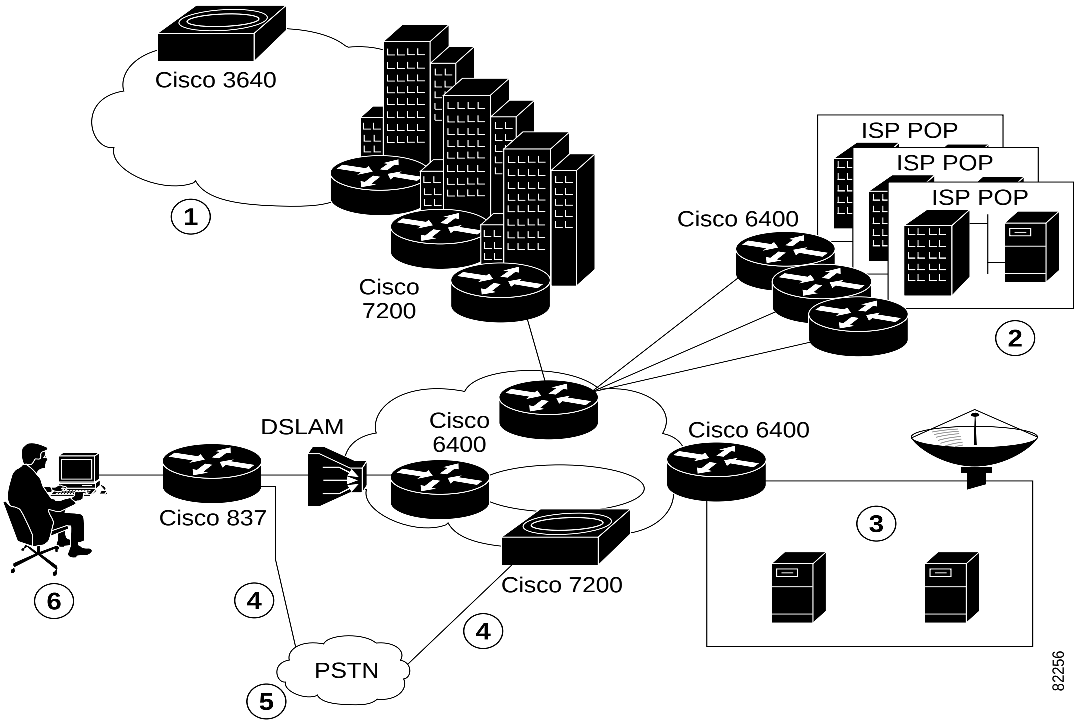
1	Corporate network connecting through a Cisco 3640 gateway	**4**	Dial backup or remote management that keeps the traffic working in case of primary line shutdown
2	Wholesale ISP business	**5**	ISDN to serve as an interface for dial backup or remote management
3	ISP POP (data center) with videoconferencing MCUs and IP/TV video servers	**6**	Small business or remote user, connecting to the network through a Cisco 836 router

Cisco 837 Router Network Connections

Figure 2-4 shows 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 2-4 Cisco 837 Router Network Connections



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

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

Internet Access Scenarios

Each network access scenario is described with a network diagram, configuration steps for setting up the network, and an example configuration.

Before You Configure Your Internet Access Network

You need to gather the following information before configuring networks based on the Internet access scenarios:

- 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 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.

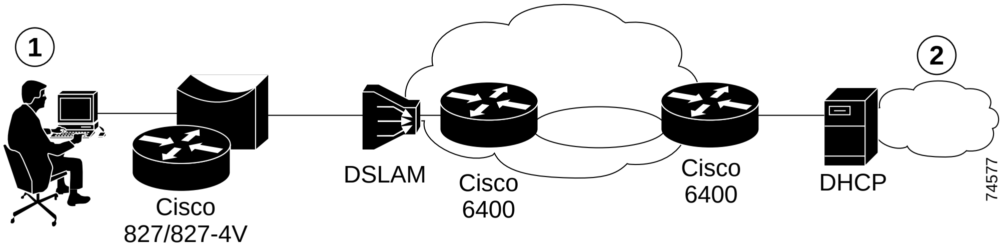
Replacing a Bridge or Modem with a Cisco 827 Router

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 2-5 shows the network topology for this scenario.

Figure 2-5 Replacing a Bridge or Modem with a Cisco 827 Router



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 6400 router onto the Internet. This network setup creates the simplicity of bridging data but also maintains router control. This network is very simple but limits more complex services such as stopping broadcast traffic. If you want more services available on your network, you may want to consider Scenario 2 or 3.

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 3, "Basic Router Configuration," and Chapter 4, "Advanced Router Configuration."

After configuring your router, you need to configure the PVC endpoint. For a general configuration example, see "Cisco 3640 Gateway Configuration Example" at the end of this chapter.

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	Purpose
Step 1	**no ip routing**	Disables IP routing.
Step 2	**bridge 1 protocol ieee**	Specifies the bridge protocol to define the type of Spanning-Tree protocol.
Step 3	**interface ethernet 0**	Enters configuration mode for the Ethernet interface.
Step 4	**bridge-group 1**	Specifies the bridge-group number to which the Ethernet interface belongs.
Step 5	**no shutdown**	Enables the Ethernet interface.
Step 6	**exit**	Exits configuration mode for the Ethernet interface and the router.
Step 7	**interface ATM 0**	Enters configuration mode for the ATM interface.
Step 8	**pvc 8/35**	Creates an ATM permanent virtual circuit (PVC) for each end node with which the router communicates.
Step 9	**encapsulation aal5snap**	Specifies the encapsulation type for the PVC.
Step 10	**bridge-group 1**	Specifies the bridge-group number to which the ATM interface belongs.
Step 11	**no shutdown**	Enables the ATM interface.
Step 12	**exit**	Exits the configuration mode for the ATM interface.

Configuration Example

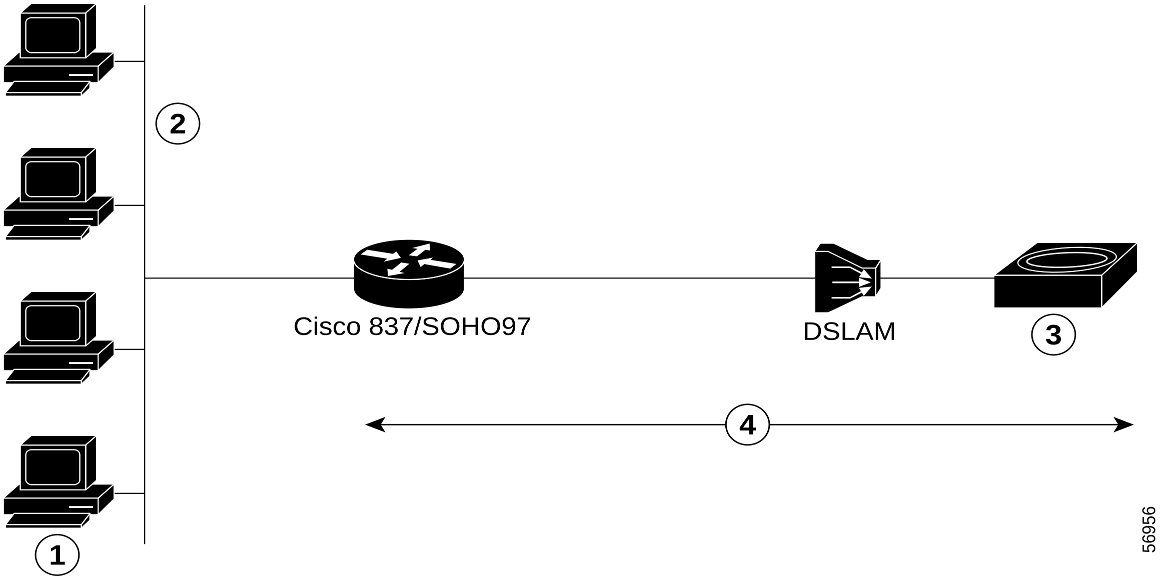
The following is a configuration example for this network scenario. You do not have to enter the commands marked "default." These commands appear automatically in the configuration file generated when you use the **show running-config** command.

```
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 837 and SOHO 97 routers support a PPP-over-Ethernet (PPPoE) client, with Network Addressing Translation (NAT) and with multiple PCs on the LAN. Figure 2-6 shows a typical deployment scenario for PPPoE support.

Figure 2-6 PPPoE Deployment Scenario



1	Multiple PCs in LAN	**3**	Access concentrator, concentrating data and LAN into ATM service over E1/T1 links
2	Multiple PCs connected in a LAN	**4**	PPPoE session. A PPPoE session is initiated on the client side by the Cisco 837 and SOHO 97 routers

A PPPoE session is initiated on the client side by the Cisco 837 or 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.

	Command	Purpose
Step 1	**vpdn enable**	Enables VPDN.
Step 2	**vpdn group** *tag*	Sets the VPDN group.
Step 3	**request-dialin**	Specifies the dialing direction.
Step 4	**protocol pppoe**	Specifies the protocol type for the VPDN.
Step 5	**interface ATM0** **mtu** *1492* **pvc** *8/35*	Enters configuration mode for the ATM interface. Sets the maximum transmission unit (MTU) size and PVC number.
Step 6	**pppoe-client dial-pool-number 1**	Defines the PPPoE client in dial pool number 1.
Step 7	**interface Dialer 1 ip address negotiated encapsulation ppp dialer-pool** *1*	Enters configuration mode for the Dialer 1 interface to obtain the IP address via IPCP. Specifies 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	Purpose
Step 1	**interface atm 0**	Enters configuration mode for the ATM interface.
Step 2	**dsl linerate** {*number* | **auto**}	Specifies 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**	Sets the IP address and subnet mask for the ATM interface.
Step 4	**pvc** *vpi/vci*	Creates an ATM PVC for each end node with which the router communicates.
Step 5	**ppoe-client dial-pool-number 1**	Binds the dialer to the interface.
Step 6	**no shutdown**	Enables the ATM 0 interface.

Configuring the Dialer Interface

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

	Command	Purpose
Step 1	**ip route** *default-gateway-ip-address mask* **dialer** *0*	Sets the IP route for the default gateway for the Dialer 0 interface.
Step 2	**interface dialer 0**	Enters the Dialer 0 interface configuration.
Step 3	**ip address negotiated**	Specifies that the IP address is to be negotiated over PPP.
Step 4	**ip mtu 1492**	Sets the size of the IP maximum transmission unit (MTU).
Step 5	**encapsulation ppp**	Sets the encapsulation type to PPP.
Step 6	**dialer pool 1**	Specifies the dialer pool to be used.
Step 7	**dialer-group 1**	Assigns this interface to a dialer list.
Step 8	**ppp authentication chap**	Sets the PPP authentication method to Challenge Handshake Authentication Protocol (CHAP).
Step 9	**exit**	Exits the Dialer 0 interface configuration.
Step 10	**dialer-list 1 protocol ip permit**	Creates 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, Cisco 836, Cisco 837, Cisco SOHO 91, Cisco SOHO 96, and Cisco SOHO 97 routers support a PPP-over-Ethernet (PPPoE) client, using a dial-on-demand PPP-over-Ethernet connection. For deployment scenario, see Figure 2-6 on page 2-8.

Configuring the Virtual Private Dial-Up Network Group Number

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

	Command	Purpose
Step 1	**vpdn enable**	Enables VPDN.
Step 2	**vpdn group** *tag*	Sets the VPDN group.
Step 3	**request-dialin**	Specifies the dialing direction.
Step 4	**protocol pppoe**	Specifies 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	Purpose
Step 1	**interface atm 0**	Enters configuration mode for the ATM interface.
Step 2	**ip address 200.200.100.1 255.255.255.0**	Sets the IP address and subnet mask for the ATM interface.

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

Configuring the Dialer Interface

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

	Command	Purpose
Step 1	**ip route** *default-gateway-ip-address mask* **dialer** *0*	Sets the IP route for the default gateway for the Dialer 0 interface.
Step 2	**interface dialer 0**	Enters Dialer 0 interface configuration.
Step 3	**ip address negotiated**	Specifies that the IP address is to be negotiated over PPP.
Step 4	**ip mtu** *1492*	Sets the size of the IP maximum transmission unit (MTU).
Step 5	**ip nat outside**	Establishes the Dialer 0 interface as the outside interface.
Step 6	**encapsulation ppp**	Sets the encapsulation type to PPP.
Step 7	**dialer pool 1**	Specifies the dialer pool to be used.
Step 8	**dialer-group 1**	Assigns this interface to a dialer list.
Step 9	**ppp authentication chap**	Sets the PPP authentication method to Challenge Handshake Authentication Protocol (CHAP).
Step 10	**exit**	Exits the Dialer 0 interface configuration.
Step 11	**dialer-list 1 protocol ip permit**	Creates 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
!
```

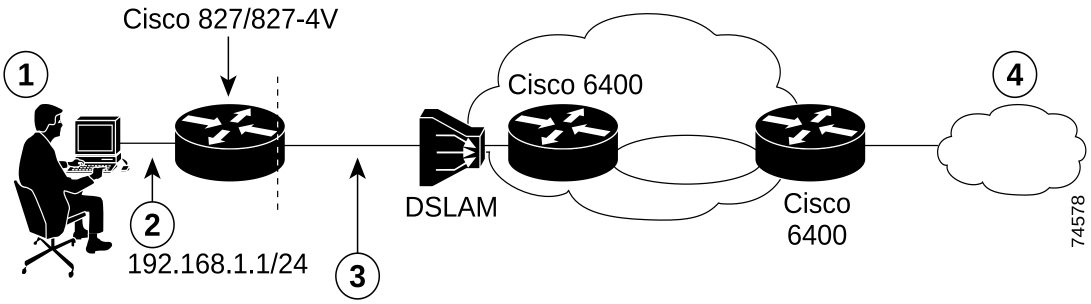
```
interface atm0
no ip address
no atm ilmi-keepalive
pvc 1/100
pppoe-client dial-pool-number 1 dial-on-demand
!
interface dialer 1
ip address negotiated
ppp authentication chap
dialer pool 1
dialer-group 1
!
dialer-list 1 protocol ip permit
```

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 gives straight user verification as you would get in a dial network.

Figure 2-7 shows the network topology for this scenario.

Figure 2-7 PPP over ATM with NAT



1	Small business or remote user	**3**	PPP over ATM PVC 8/35
2	Connection to Ethernet 0 address 192.168.1.1/24 through a dialer interface	**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 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 Dialer Interface
- Configuring the ATM Interface

- Configuring NAT
- Configuration Example

To add additional features to this network, seeChapter 3, “Basic Router Configuration” and Chapter 4, “Advanced Router Configuration.”

After configuring your router, you need to configure the PVC endpoint. For a general configuration example, see“Cisco 3640 Gateway Configuration Example” at the end of this chapter.

Configuring the Ethernet interface

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

	Command	Purpose
Step 1	**interface ethernet 0**	Enters configuration mode for the Ethernet interface.
Step 2	**ip address 192.168.1.1 255.255.255.0**	Sets the IP address and subnet mask for the Ethernet interface.
Step 3	**no shutdown**	Enables the interface and configuration changes just made to the Ethernet interface.
Step 4	**exit**	Exits 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	Purpose
Step 1	**interface dialer 0**	Enters configuration mode for the dialer interface.
Step 2	**ip address negotiated**	Configures a negotiated IP address.
Step 3	**ip nat outside**	Sets the interface to be connected to the outside network.
Step 4	**encapsulation ppp**	Specifies the encapsulation type for the PVC to be PPP.
Step 5	**dialer pool 1**	Specifies which dialer pool number you are using.
Step 6	**exit**	Exits 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	Purpose
Step 1	**interface ATM 0**	Enters configuration mode for the ATM interface.
Step 2	**pvc 8/35**	Creates an ATM PVC for each end node with which the router communicates.

	Command	Purpose
Step 3	**encapsulation aal5mux ppp dialer**	Specifies the encapsulation type for the PVC to be aal5mux (PPP) and point back to the dialer interface.
Step 4	**dialer pool-member 1**	Specifies a dialer pool-member.
Step 5	**no shutdown**	Enables interface and configuration changes just made to the ATM interface.
Step 6	**exit**	Exits configuration mode for the ATM interface.

Configuring NAT

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

	Command	Purpose
Step 1	**ip nat inside source list 1 interface dialer 0 overload**	Enables 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**	Sets 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**	Defines a standard access list permitting addresses that need translation.
Step 4	**interface ethernet 0**	Enters configuration mode for the Ethernet interface.
Step 5	**ip nat inside**	Establishes the Ethernet interface as the inside interface.
Step 6	**no shutdown**	Enables interface and configuration changes just made to the Ethernet interface.
Step 7	**exit**	Exits 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 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

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.

Like the Cisco 831 and Cisco 837 routers and the Cisco SOHO 91 and Cisco SOHO 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 Cisco 837 routers and the Cisco SOHO 91 and Cisco SOHO 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 in the "Configuring Dial Backup and Remote Management for the Cisco 837 and Cisco SOHO 97 Routers" section on page 2-19 refers to backup remote management, the function that 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, Cisco 836, and Cisco 837 routers and the Cisco SOHO 91, Cisco SOHO 96, and Cisco SOHO 97 routers.

Cisco 836 and Cisco 837 Routers and Cisco SOHO 96 and Cisco SOHO 97 Routers

The following can be used to bring up the dial backup feature in the Cisco IOS software for the Cisco 836 and Cisco 837 routers and the Cisco SOHO 96 and Cisco SOHO 97 routers:

- Backup Interfaces
- Floating Static Routes
- Dialer Watch

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 Cisco 837 routers, the dial backup feature is supported for the encapsulations identified in Table 2-1.

Table 2-1 Encapsulation Types Supported by Dial Backup Feature on the Cisco 836 and Cisco 837 Routers

Encapsulation Type (WAN)	Dial Backup Possible	Type of Dial Backup Method	Limitations
PPP over ATM PPP over Ethernet	Yes	• Backup interface method • Floating static routes • 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. 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 • Floating static routes • 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 2-2 shows the encapsulation types supported by the Cisco 831 router dial backup.

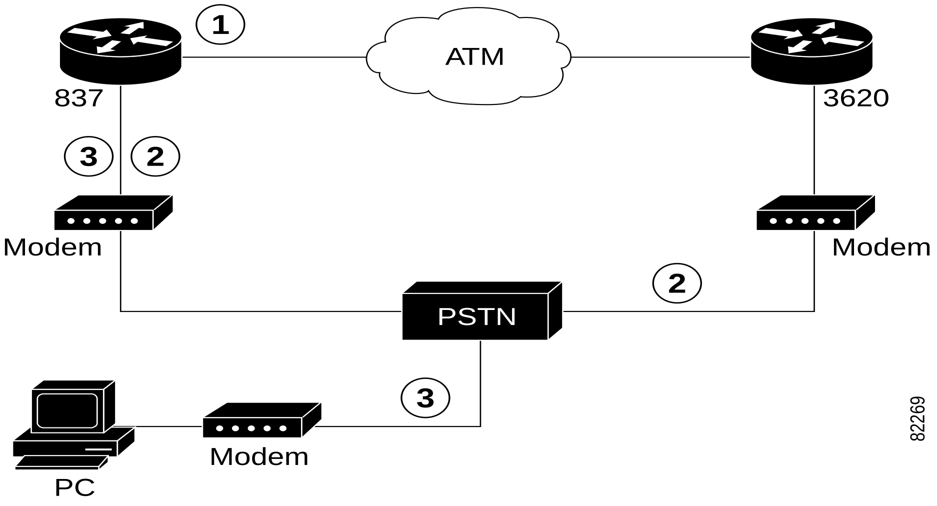
Table 2-2 Encapsulation Types Supported by Dial Backup for the Cisco 831 Router

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 2-8 shows how dial backup and remote management work in a network system when the primary line goes down.

Figure 2-8 Cisco 837 Router Dial Backup and Remote Management

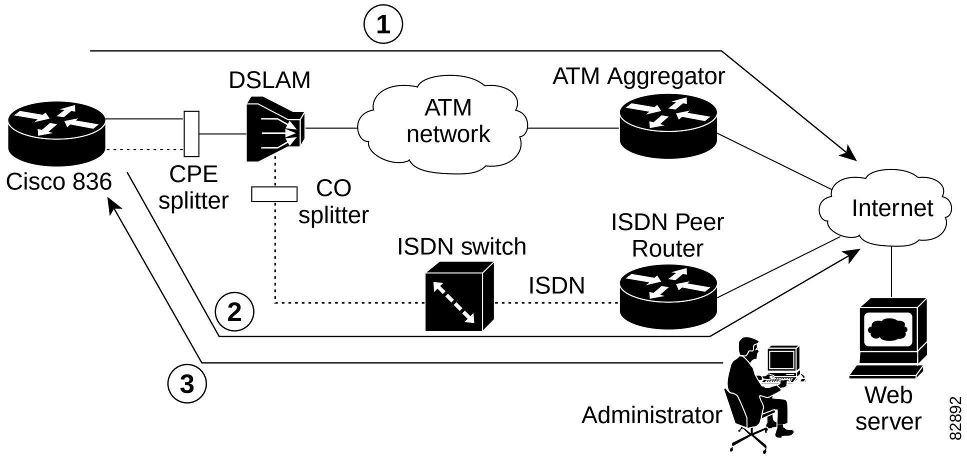


1	Main WAN link; primary connection to Internet service provider
2	Dial backup; serves as a failover link when primary line goes down
3	Remote management; serves as dial-in access to allow changes or updates to Cisco IOS configurations

Configuring Dial Backup and Remote Management for the Cisco 836 and Cisco SOHO 96 Routers

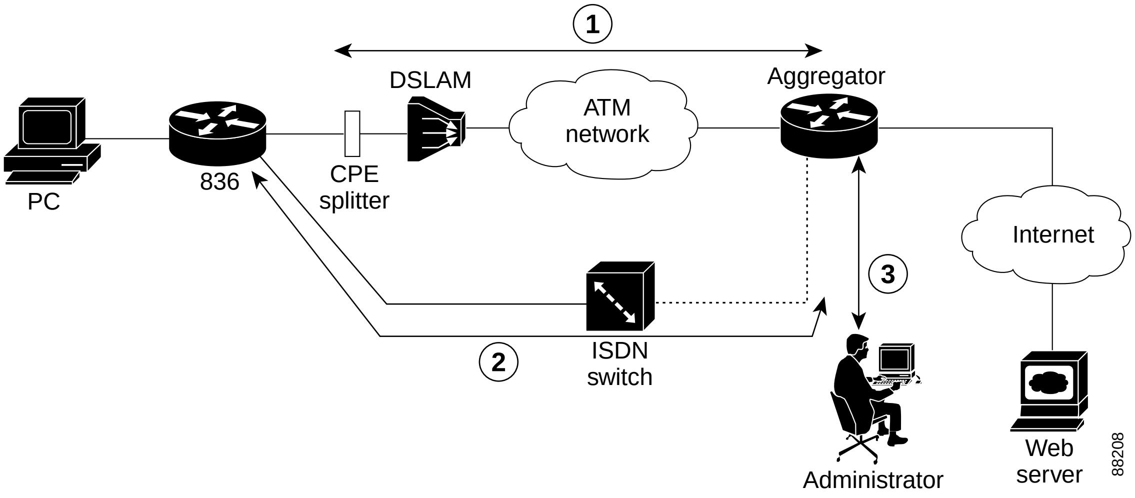
Figure 2-9 and Figure 2-10 show how dial backup and remote management work in a network system when the primary line goes down. Two scenarios are typical applications of the Cisco 836 and the Cisco SOHO 96 routers. In Figure 4-9, the dial backup link goes through CPE splitter, DSLAM, and CO splitter 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 2-9 Cisco 836 Router Dial Backup and Remote Management—Dial Backup Through CPE Splitter, DSLAM, and CO Splitter



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 2-10 Cisco 836 Router Dial Backup and Remote Management—Dial Backup Directly from Router to ISDN Switch



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	Purpose
Step 1	**ip name-server** *206.13.28.12*	Enters your ISP DNS IP address.
Step 2	**ip dhcp pool** *1*	Configures CPE as a local DHCP server.
Step 3	**vpdn enable**	Enables VPDN.
Step 4	**vpdn-group** *1*	Specifies VPDN group for protocol PPPoE.
Step 5	**chat-script Dialout ABORT ERROR ABORT BUSY "" "AT" OK "ATDT** *5555102* **T" TIMEOUT 45 CONNECT \c**	Configures a chat script for a modem.
Step 6	**interface Async1**	Enters configuration mode for the async interface.
Step 7	**interface Dialer***3*	Enters configuration mode for the dialer interface.

	Command	Purpose
Step 8	**dialer watch-group** *1*	Specifies the group number for watch-list.
Step 9	**ip nat inside source list 101 interface Dialer3 overload**	Establishes the Ethernet interface as the inside interface.
Step 10	**ip route 0.0.0.0 0.0.0.0 !** (*dial backup peer address @ISP*)	Sets 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*	Defines an extended access list permitting addresses that need translation.
Step 12	**dialer watch-list 1 ip !** *(ATM peer address @ISP) 255.255.255.255*	Evaluates the status of the primary link, based on the existence of routes to the peer.
Step 13	**line con 0**	Enters configuration mode for the console interface.
Step 14	**modem enable**	Changes the console port to auxiliary port function.
Step 15	**line aux 0**	Enters configuration mode for the auxiliary interface.
Step 16	**flow control hardware**	Enables 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-timedout 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 2-25 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	Purpose
Step 1	**isdn switch-type basic-net3**	Specifies the ISDN switch type.
Step 2	**interface BRI0**	Enters configuration mode for the ISDN Basic Rate Interface (BRI).
Step 3	**encapsulation ppp**	Sets BRI0 interface encapsulation type to PPP.
Step 4	**dialer pool-member** *1*	Specifies the dialer pool membership.
Step 5	**isdn switch-type basic-net3**	Specifies the ISDN switch type.
Step 6	**exit**	Exits to return to global configuration mode.
Step 7	**interface Dialer0**	Enters configuration mode for the dialer interface.
Step 8	**ip address negotiated**	Obtains the IP address from the peer.
Step 9	**encapsulation ppp**	Specifies Dialer 0 encapsulation type as PPP.
Step 10	**dialer pool 1**	Specifies 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**	Specifies the telephone number to be dialed.
Step 12	**dialer-group 1**	Assigns this interface to a dialer group.

	Command	Purpose
Step 13	**exit**	Exits to return to global configuration mode.
Step 14	**dialer-list 1 protocol ip permit**	Creates 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 2-16, 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	Purpose
Step 1	**interface ATM0**	Enters ATM interface configuration mode.
Step 2	**backup interface BRI0**	Assigns 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	Purpose
Step 1	**ip route 0.0.0.0 0.0.0.0 22.0.0.2**	Assigns the primary route.
Step 2	**ip route 0.0.0.0 0.0.0.0 192.168.2.2 150**	Assigns 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	Purpose
Step 1	**router rip**	Enables RIP routing.
Step 2	**network 22.0.0.0**	Defines 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**	Assigns 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 steps in the table below to configure the dialer watch on the Cisco 836 router's ISDN port, beginning in global configuration mode.

	Command	Purpose
Step 1	**interface Dialer0**	Enters configuration mode for the dial backup interface.
Step 2	**dialer watch-group 1**	Specifies the group number for the watch list.
Step 3	**exit**	Exits to return to global configuration mode.
Step 4	**ip route 0.0.0.0 0.0.0.0 22.0.0.2**	Assigns 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**	Assigns 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**	Assigns 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 protocol 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 in this chapter.

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	Purpose
Step 1	**interface Async1**	Enters configuration mode for the async interface.
Step 2	**line con 0**	Enters configuration mode for the console interface.
Step 3	**modem enable**	Changes the console port to the auxiliary port.
Step 4	**line aux 0**	Enters configuration mode for the auxiliary interface.
Step 5	**flowcontrol hardware**	Enables 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.

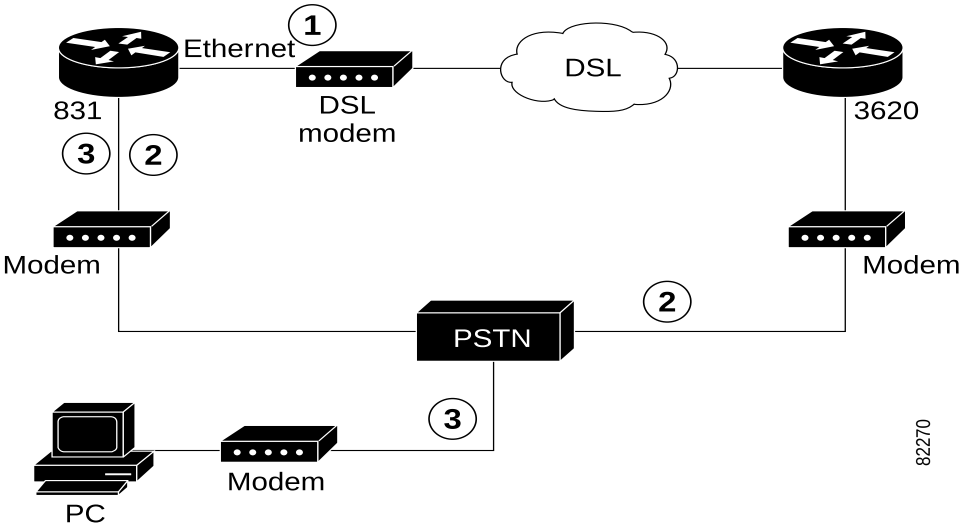
```
!
!Remote management account
username dialin password cisco
modemcap entry MY_USR_MODEM:MSC=&F1S0=1
```

```
!
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 2-11 shows 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 2-11 Cisco 831 Router Dial Backup and Remote Management in a DSL Modem Environment



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	Purpose
Step 1	**ip name-server** *206.13.28.12*	Enters your ISP DNS IP address.
Step 2	**ip dhcp pool** *1*	Configures CPE as a local DHCP server.
Step 3	**vpdn enable**	Enables VPDN.
Step 4	**vpdn-group** *1*	Specifies VPDN group for protocol PPPoE.
Step 5	**chat-script Dialout ABORT ERROR ABORT BUSY "" "AT" OK "ATDT** *5555102* **T" TIMEOUT 45 CONNECT \c**	Configures a chat script for a modem.
Step 6	**interface Async1**	Enters configuration mode for the async interface.
Step 7	**interface Dialer***3*	Enters configuration mode for the dialer interface.

	Command	Purpose
Step 8	**ip nat inside source list 101 interface Dialer3 overload**	Establishes the Ethernet interface as the inside interface.
Step 9	**ip route 0.0.0.0 0.0.0.0 !** *(dial backup peer address @ISP)*	Sets 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*	Defines an extended access list permitting addresses that need translation.
Step 11	**dialer watch-list 1 ip !** *(peer address @ISP) 255.255.255.255*	Evaluates the status of the primary link, based on the existence of routes to the peer.
Step 12	**line con 0**	Enters configuration mode for the console interface.
Step 13	**modem enable**	Changes the console port to the auxiliary port.
Step 14	**line aux 0**	Enters configuration mode for the auxiliary interface.
Step 15	**flowcontrol hardware**	Enables 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	Purpose
Step 1	**interface Async1**	Enters configuration mode for the async interface.
Step 2	**line con 0**	Enters configuration mode for the console interface.
Step 3	**modem enable**	Changes the console port to the auxiliary port.
Step 4	**line aux 0**	Enters configuration mode for the auxiliary interface.
Step 5	**flowcontrol hardware**	Enables 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 to set all but one interface to ignore Network Registrar.

```
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	Purpose
Step 1	**interface ethernet 0**	Enters configuration mode for the Ethernet interface.
Step 2	**ip address** *ip-address mask*	Sets the IP address and subnet mask for the Ethernet interface.
Step 3	**no shutdown**	Enables the Ethernet interface to change the state from administratively down to up.
Step 4	**exit**	Exits configuration mode for the Ethernet interface.

For complete information on the Ethernet commands, see the Cisco IOS Release 12.2 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 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.

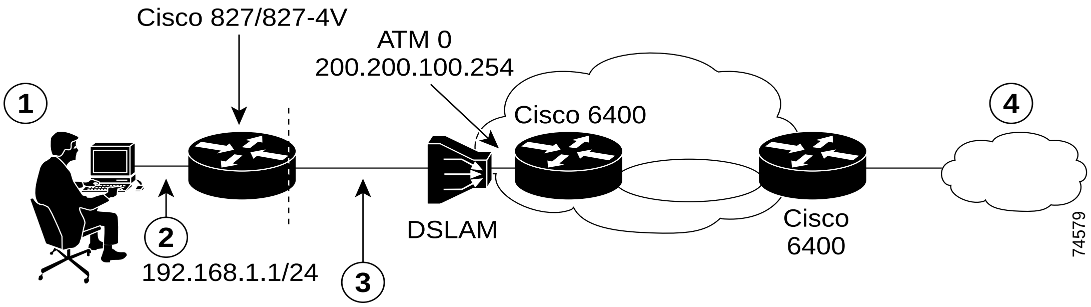
For instructions on configuring a RADIUS client, see the *Cisco IOS Security Configuration Guide*.

RFC 1483 Encapsulation with NAT

This network 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, since there is slightly less overhead than PPP.

Figure 2-12 shows the network topology for this scenario.

Figure 2-12 RFC 1483 Encapsulation with NAT



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 3, “Basic Router Configuration,” and Chapter 4, “Advanced Router Configuration.”

After configuring your router, you need to configure the PVC endpoint. For a general configuration example, see “Cisco 3640 Gateway Configuration Example” at the end of this chapter.

Configuring the Ethernet Interface

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

	Command	Purpose
Step 1	**interface ethernet 0**	Enters configuration mode for the Ethernet interface.
Step 2	**ip address 192.168.1.1 255.255.255.0**	Sets the IP address and subnet mask for the Ethernet interface.
Step 3	**no shutdown**	Enables the Ethernet interface.
Step 4	**exit**	Exits configuration mode for the Ethernet interface.

Configuring the ATM Interface

Use this table to configure the ATM interface, beginning in global configuration mode.

	Command	Purpose
Step 1	**interface ATM 0**	Enters configuration mode for the ATM interface.
Step 2	**ip address 200.200.100.1 255.255.255.0**	Sets the IP address and subnet mask for the ATM interface.
Step 3	**pvc 8/35**	Creates an ATM PVC for each end node with which the router communicates.
Step 4	**protocol ip 200.200.100.254 broadcast**	Sets the protocol broadcast for the IP address.
Step 5	**encapsulation** *type*	Specifies the encapsulation type for the PVC to be AAL5SNAP or AAL5MUX IP.
Step 6	**no shutdown**	Enables the ATM interface.
Step 7	**exit**	Exits configuration mode for the ATM interface.

Configuring NAT

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

	Command	Purpose
Step 1	**ip nat inside source list 1 pool interface ATM0 overload**	Enables 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**	Sets 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**	Defines a standard access list permitting addresses that need translation.
Step 4	**interface ethernet 0**	Enters configuration mode for the Ethernet interface.

	Command	Purpose
Step 5	**ip nat inside**	Establishes the Ethernet interface as inside interface.
Step 6	**exit**	Exits configuration mode for the Ethernet interface.
Step 7	**interface atm 0**	Enters configuration mode for the ATM interface.
Step 8	**ip nat outside**	Establishes the ATM interface as outside interface.
Step 9	**exit**	Exits 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 generated when you use the **show running-config** command.

The following is an RFC 1483 LLC/SNAP encapsulation over ATM configuration example.

```
!
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 RFC 1483 VC-MUX configuration example.

```
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
```

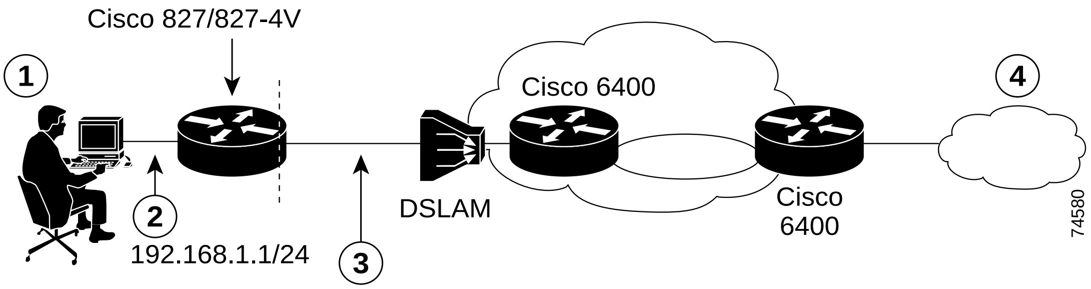
Integrated Routing and Bridging

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 with a router enables feature additions 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 2-13 shows an IRB scenario.

Figure 2-13 IRB Internet Scenario



1	Small business or remote user	**3**	Connection to Ethernet 0 address 192.168.1.1/24
2	ATM 0 PVC 8/35	**4**	The Internet

One side of the network (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, and the number of PVCs is set by default.

NAT, represented as the dashed line at the edge of the Cisco 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 Default Gateway
- Configuring the Ethernet Interface and IRB
- Configuring the ATM Interface
- Configuring the BVI
- Configuring NAT
- Configuration Example

To add additional features to this network, see Chapter 3, “Basic Router Configuration,” and Chapter 4, “Advanced Router Configuration.”

After configuring your router, you need to configure the PVC endpoint. For a general configuration example, see “Cisco 3640 Gateway Configuration Example” at the end of this chapter.

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

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

	Command	Purpose
Step 1	**bridge irb**	Specifies IRB.
Step 2	**bridge 1 route ip**	Enables IP routing to and from bridge-group 1.
Step 3	**bridge 1 protocol ieee**	Specifies the bridge protocol to define the type of Spanning-Tree Protocol (STP).
Step 4	**interface ethernet 0**	Enters configuration mode for Ethernet interface.
Step 5	**ip address 192.168.1.1 255.255.255.0**	Sets the IP address and subnet mask for the Ethernet interface.
Step 6	**no shutdown**	Enables the Ethernet interface.
Step 7	**exit**	Exits configuration mode for Ethernet interface.

Configuring the ATM Interface

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

	Command	Purpose
Step 1	**interface ATM 0**	Enters configuration mode for the ATM interface.
Step 2	**pvc 8/35**	Creates an ATM PVC for each end node with which the router communicates.
Step 3	**encapsulation aal5snap**	Specifies the encapsulation type for the PVC.

	Command	Purpose
Step 4	**bridge-group 1**	Specifies the bridge-group number to which the ATM interface belongs.
Step 5	**no shutdown**	Enables the ATM interface.
Step 6	**exit**	Exits configuration mode for the ATM interface.

Configuring the BVI

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

	Command	Purpose
Step 1	**interface bvi 1**	Enters configuration mode for the BVI.
Step 2	**ip address 200.200.100.1 255.255.255.0**	Sets the IP address and subnet mask for the BVI.
Step 3	**exit**	Exits configuration mode for Ethernet interface.

Configuring NAT

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

	Command	Purpose
Step 1	**ip nat pool test 200.200.100.1 200.200.100.1 255.255.255.0**	Creates pool of global IP addresses for NAT.
Step 2	**access-list 101 permit ip 192.168.1 0.0.0.0.255 any log**	Defines a standard access list permitting addresses that need translation.
Step 3	**ip nat inside source list 101 pool test overload**	Enables dynamic translation of addresses permitted by access list to one of addresses specified in pool.
Step 4	**interface ethernet 0**	Enters configuration mode for the Ethernet interface.
Step 5	**ip nat inside**	Establishes the Ethernet interface as the inside interface.
Step 6	**no shutdown**	Enables interface and configuration changes just made to the interface.
Step 7	**exit**	Exits configuration mode for the Ethernet interface.
Step 8	**interface ATM 0**	Enters configuration mode for the ATM interface.
Step 9	**ip nat outside**	Establishes the ATM interface as the outside interface.
Step 10	**no shutdown**	Enables interface and configuration changes just made to the interface.
Step 11	**exit**	Exits configuration mode for the ATM interface.
Step 12	**interface bvi 1**	Enters configuration mode for the BVI.
Step 13	**ip nat outside**	Establishes the BVI as the outside interface.

	Command	Purpose
Step 14	**no shutdown**	Enables interface and configuration changes just made to the interface.
Step 15	**end**	Exits 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 generated when you use the **show running-config** command.

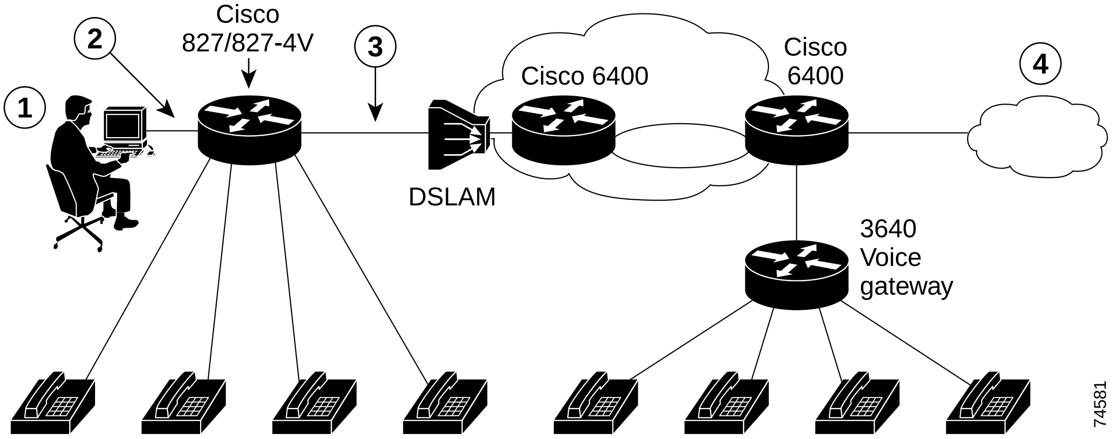
```
bridge irb
!
interface Ethernet0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast (default)
ip nat inside
!
interface ATM0
no ip address
no ip directed-broadcast (default)
ip nat outside
no atm ilmi-keepalive (default)
pvc 8/35
encapsulation aal5snap
!
bridge-group 1
!
interface BVI1
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 each of them separate. 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 2-14 shows a CRB Internet scenario with the voice traffic routed and the data traffic bridged. Both the Cisco 827/827-4V router and the Cisco 3640 voice gateway are supporting voice traffic from telephones.

Figure 2-14 CRB Internet Scenario



1	Small business or remote user	**3**	ATM connection, ATM0.1 PVC 1/40 Voice 1.0.0.1/24, ATM0.2 PVC 8/35 data
2	Ethernet 0 bridge	**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 subinterface2, 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 virtual path identifier and virtual channel identifier (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 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 3, “Basic Router Configuration” and Chapter 4, “Advanced Router Configuration.”

After configuring your router, you need to configure the PVC endpoint. For a general configuration example, see “Cisco 3640 Gateway Configuration Example” at the end of this chapter.

Specifying CRB and Configuring the Ethernet Interface

Follow these steps to specify CRB and configure the Ethernet interface, beginning in global configuration mode.

	Command	Purpose
Step 1	**bridge crb**	Specifies CRB.
Step 2	**interface ethernet 0**	Enters configuration mode for the Ethernet interface.
Step 3	**bridge-group 1**	Specifies the bridge-group number to which the Ethernet interface belongs.
Step 4	**exit**	Exits configuration mode for the Ethernet interface and the router.
Step 5	**bridge 1 protocol ieee**	Specifies the bridge protocol to define the type of STP.

Configuring the ATM Interface and Subinterfaces

Follow these steps to configure the ATM interface and subinterfaces, beginning in global configuration mode.

	Command	Purpose
Step 1	**interface ATM 0.1 point-to-point**	Specifies the ATM0.1 subinterface.
Step 2	**ip address 1.0.0.1 255.255.255.0**	Sets the IP address and subnet mask for the ATM0.1 subinterface.
Step 3	**pvc 1/40**	Creates an ATM PVC for each end node with which the router communicates.
Step 4	**encapsulation aal5snap**	Specifies the encapsulation type for the PVC.
Step 5	**protocol ip 1.0.0.2 broadcast**	Sets the protocol broadcast for the IP address.
Step 6	**interface ATM 0.2 point-to-point**	Specifies the ATM0.2 subinterface.
Step 7	**pvc 8/35**	Creates an ATM PVC for each end node with which the router communicates.
Step 8	**encapsulation aal5snap**	Specifies the encapsulation type for the PVC.
Step 9	**bridge-group 1**	Specifies the bridge-group number to which the Ethernet interface belongs.
Step 10	**no shutdown**	Enables the ATM interface.
Step 11	**exit**	Exits 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

Follow the steps below to configure the POTS dial peers, beginning in global configuration mode. Table 2-3 shows the destination telephone number and port for each dial peer POTS port.

	Command	Purpose
Step 1	**dial-peer voice** *number* **POTS**	Enters configuration mode for the dial peer.
Step 2	**destination-pattern** *string*	Defines the telephone number associated with the port.
Step 3	**voice port-number**	Specifies the port number.

Table 2-3 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

Use this table to configure VoIP dial peers for H.323 signaling, beginning in global configuration mode. Table 2-4 shows the destination telephone number for each voice dial peer.

	Command	Purpose
Step 1	**dial-peer voice** *number* **VoIP**	Enters configuration mode for the dial peer.
Step 2	**destination-pattern** *string*	Defines the destination telephone number associated with each VoIP dial peer.
Step 3	**codec g711ulaw**	Specifies a codec if you are not using the default codec of g.729.
Step 4	**session target ipv4:1.0.0.2**	Specifies a destination IP address for each dial peer.

Table 2-4 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 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

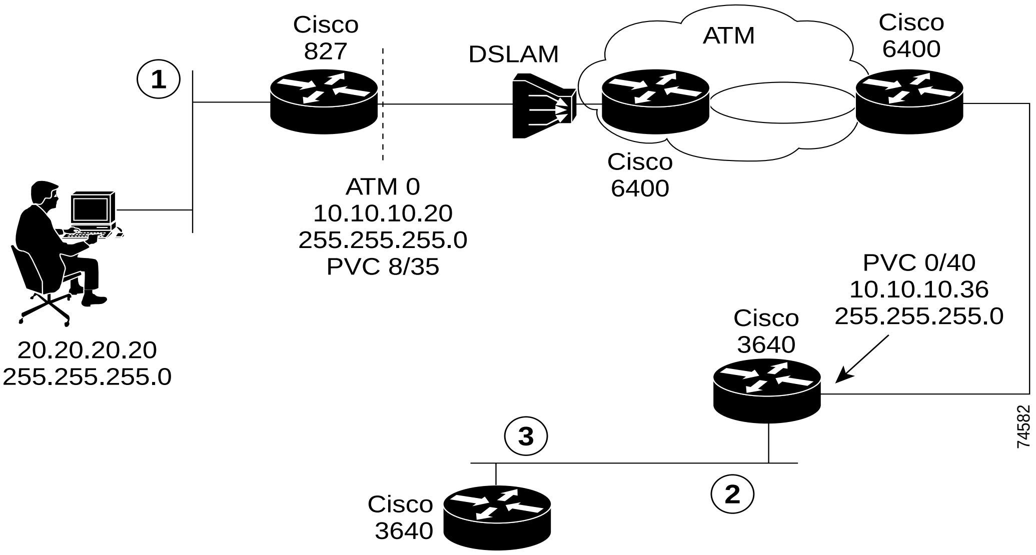
This section describes a voice scenario configuration using the Cisco 827-4V router in an H.323 signaling environment.

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 discussed below.

Data Network

Figure 2-15 shows a data network with traffic routing through the Cisco 827 router and then switching onto the ATM interface.

Figure 2-15 Data Network



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 and it is associated with a QoS policy called *mypolicy*. Data traffic coming from the Ethernet must have an IP precedence below 5 (critical) to distinguish it from voice traffic.

Enhanced IGRP 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, Enhanced IGRP assumes that the state of a destination has changed and sends an incremental update.

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

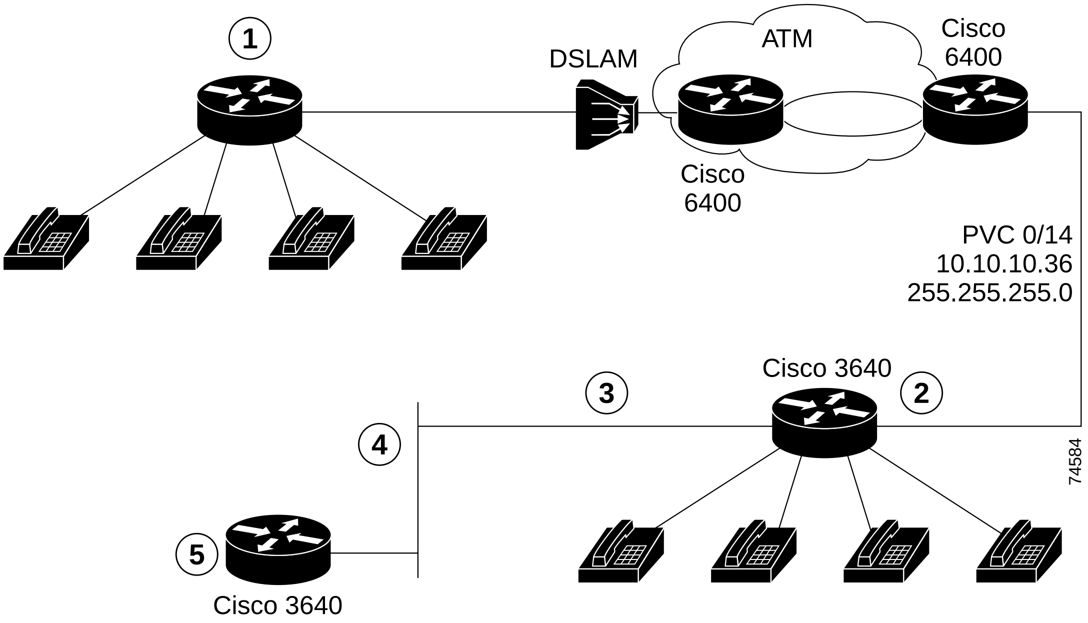
This scenario includes configuration tasks and a configuration example. To add additional features to this network, see Chapter 3, "Basic Router Configuration" and Chapter 4, "Advanced Router Configuration."

After configuring your router, you need to configure the PVC endpoint. For a general configuration example, see "Cisco 3640 Gateway Configuration Example" at the end of this chapter.

Voice Network

Figure 2-16 shows a voice network with a Cisco 827-4V router and a Cisco 3640 router as the VoIP *gateway* using H.323 signaling (H.323 gateway).

Figure 2-16 Voice Network



1	Cisco 827-4V router serving as a voice gateway	**4**	Ethernet 1 connection at address 172.17.1.1, subnet 255.255.255.0
2	Cisco 3640 router serving as a voice gateway	**5**	Cisco 3640 router serving as voice gatekeeper
3	Ethernet 0 connection at address 172.17.1.36, subnet 255.255.255.0		

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 and the 3640 router are in the same zone.

Dialed numbers are stored by the VoIP session application in the Cisco 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 routes 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 configure the data network and then the voice network.

- Configure the data network:
  - Configuring the class map, route map, and policy map
  - Configuring the Ethernet interface
  - Configuring the ATM interface
  - Configuring Enhanced IGRP
- Configure the voice network:
  - Configuring the POTS dial peers
  - Configuring VoIP dial peers for H.323 signaling
- Configuration Examples

Use the tables shown here to configure this scenario. Each command includes the values in the data and voice configuration examples shown at the end of this section. 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 "Cisco 3640 Gateway Configuration Example" at the end of this chapter.

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	Purpose
Step 1	**access-lists 101 permit ip any any precedence 5**	Configures the access list.
Step 2	**class-map voice**	Configures the class map.
Step 3	**match access-group 101**	Assigns access list 101 to the class map.
Step 4	**route-map data permit 10**	Configures the route map.
Step 5	**ip precedence routine**	Sets the IP precedence.
Step 6	**policy-map mypolicy**	Configures a policy map.
Step 7	**class voice**	Specifies the class for queuing voice traffic.
Step 8	**priority 176**	Specifies the bandwidth for queuing.[1]
Step 9	**class class-default**	Configures 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 here to configure the Ethernet interface, beginning in global configuration mode.

	Command	Purpose
Step 1	**interface ethernet 0**	Enters configuration mode for the Ethernet interface.
Step 2	**ip address 20.20.20.20 255.255.255.0**	Sets the IP address and subnet mask for the Ethernet interface.
Step 3	**ip policy route-map data**	Configures the IP policy route map.
Step 4	**ip route-cache policy**	Enables fast-switching policy routing.
Step 5	**no shutdown**	Enables the Ethernet interface.
Step 6	**exit**	Exits configuration mode for the Ethernet interface.

Configuring the ATM Interface

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

	Command	Purpose
Step 1	**interface ATM 0**	Enters configuration mode for the ATM interface.
Step 2	**ip address 10.10.10.20 255.255.255.0**	Sets the IP address and subnet mask for the ATM interface.
Step 3	**pvc 8/35**	Creates an ATM PVC for each end node with which the router communicates.
Step 4	**encapsulation aal5snap**	Specifies the encapsulation type for the PVC.
Step 5	**protocol ip 10.10.10.36 broadcast**	Specifies the protocol broadcast for the IP address.
Step 6	**service-policy output mypolicy**	Specifies the service policy for the ATM interface.
Step 7	**vbr-nrt 640 640 1**	Specifies the ATM service class.
Step 8	**no shutdown**	Enables the ATM interface.
Step 9	**exit**	Exits configuration mode for the ATM interface.

Configuring Enhanced IGRP

Follow the steps here to configure Enhanced IGRP, beginning in global configuration mode.

	Command	Purpose
Step 1	**router eigrp 100**	Enters router configuration mode, and enables Enhanced IGRP on the router. The autonomous-system number identifies the route to other Enhanced IGRP routers and is used to tag the Enhanced IGRP information.
Step 2	**network** *number*	Specifies the network number for each directly connected network.
Step 3	**exit**	Exits router configuration mode.

Configuring the POTS Dial Peers

Follow the steps here to configure each POTS dial peer, beginning in global configuration mode.

	Command	Purpose
Step 1	**dial-peer voice** *number* **POTS**	Enters configuration mode for the dial peer
Step 2	**destination-pattern** *string*	Defines the destination telephone number associated with the VoIP dial peer.
Step 3	**port** *number*	Specifies the port number.

Configuring VoIP Dial Peers for H.323 Signaling

Follow the steps here to configure VoIP dial peers for H.323 signaling in global configuration mode.

	Command	Purpose
Step 1	**dial-peer voice** *number* **VoIP**	Enters configuration mode for the dial peer.
Step 2	**destination-pattern** *string*	Defines the destination telephone number associated with each VoIP dial peer.
Step 3	**codec g711ulaw**	Specifies a codec if you are not using the default codec of g.729.
Step 4	**ip precedence 5**	Sets the IP precedence.
Step 5	**session target ras**	Specifies 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 file 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 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 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
```

Basic Router Configuration

This chapter includes basic feature-by-feature configuration procedures. This chapter is useful if you have a network in place and you want to add specific basic features.

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 2, “Network Scenarios.” For advanced router configuration topics and feature descriptions, see Chapter 4, “Advanced Router Configuration.”

This chapter contains the following sections:

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:

- Order an ADSL or G.SHDSL line from your telephone service provider.
- Determine the number of PVCs 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 in Appendix A, "Cisco IOS Basic Skills." For more information on the commands used in the following tables, see the Cisco IOS Release 12.2 documentation set.

Configuring Global Parameters

Use the following table to configure the router for global parameters.

	Command	Purpose
Step 1	**configure terminal**	Enters configuration mode.
Step 2	**hostname** *name*	Specifies the name for the router.
Step 3	**enable secret** *password*	Specifies an encrypted password to prevent unauthorized access to the router.
Step 4	**ip subnet-zero**	Configures the router to recognize zero subnet range as valid range of addresses.
Step 5	**no ip domain-lookup**	Disables the router from translating unfamiliar words (typos) entered during a console session into IP addresses.

For complete information on the global parameter commands, see the Cisco IOS Release 12.2 documentation set.

Configuring the Ethernet Interface

To configure the Ethernet interface, use the following table, beginning in global configuration mode.

	Command	Purpose
Step 1	**interface ethernet 0**	Enters configuration mode for the Ethernet interface.
Step 2	**ip address** *ip-address mask*	Sets the IP address and subnet mask for the Ethernet interface.
Step 3	**no shutdown**	Enables the Ethernet interface to change the state from administratively down to up.
Step 4	**exit**	Exits configuration mode for the Ethernet interface.

For complete information on the Ethernet commands, see the Cisco IOS Release 12.2 documentation set. For more general information on Ethernet concepts, see Chapter 1, “Concepts.”

Note The SOHO 97 Router Ethernet interface remains in an up state when the connected switchport is down and when no cable is connect to the Ethernet interface. In addition, the switchport that is connected to the SOHO 97 Ethernet port stays up when the SOHO 97 Ethernet port is down.

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 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#show interface 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.

Use the following table to configure the dialer interface, beginning in global configuration mode.

	Command	Purpose
Step 1	**interface dialer** *number*	Enters configuration mode for the dialer interface.
Step 2	**encapsulation** *ppp*	Specifies the encapsulation type for the PVC as PPP.
Step 3	**ip address** *ip-address mask*	Sets the IP address and subnet mask for the dialer interface.
Step 4	**dialer pool** *number*	Specifies which dialer pool number you are using.
Step 5	**pvc** *vpi/vci*	Creates an ATM PVC for each end node with which the router communicates.
Step 6	**encapsulation aal5mux ppp dialer**	Specifies the encapsulation type as AAL5MUX PPP.
Step 7	**dialer pool-member** *number*	Specifies a dialer pool-member.
Step 8	**dialer-group** *number*	Specifies a dialer group. The dialer group is required to fast-switch outgoing packets.
Step 9	**exit**	Exits 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 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)#show interface 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, see the Cisco IOS Release 12.2 documentation set.

Configuration Tasks

Use the following table to configure the loopback interface.

	Command	Purpose
Step 1	**interface Loopback** *0*	Enters configuration mode for the loopback interface.
Step 2	**ip address** *ip-address mask*	Sets the IP address and subnet mask for the loopback interface.

	Command	Purpose
Step 3	**ip nat outside**	Sets the interface to be connected to the outside network.
Step 4	**exit**	Exits 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 #show interface loopback 0
Loopback0 is up, line protocol is up
  Hardware is Loopback
  Internet address is 200.200.100.1/24
  MTU 1514 bytes, BW 8000000 Kbit, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation LOOPBACK, loopback not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Another way to verify the loopback interface is to 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

To configure the Asynchronous Transfer Mode (ATM) interface, use the following table, 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**. See the Cisco IOS Release 12.2 documentation set. For more information on definitions of service classes, see Chapter 1, "Concepts."

	Command	Purpose
Step 1	**interface ATM** *0*	Enters configuration mode for the ATM interface.
Step 2	**dsl equipment-type** {**co** | **cpe**}	Configures the DSL equipment type, if applicable.
Step 3	**dsl linerate** {*number* | **auto**}	Specifies 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*	Sets the G.SHDSL operating mode, if applicable, and select the G.991.2 annex.
Step 5	**ip address** *ip-address mask*	Sets the IP address and subnet mask for the ATM interface.
Step 6	**pvc** *vpi/vci*	Creates an ATM PVC for each end node with which the router communicates.
Step 7	**protocol ip** *ip-address* **broadcast**	Sets the protocol broadcast for the IP address.
Step 8	**encapsulation** *protocol*	Specifies the encapsulation type for the PVC. Encapsulations can be specified as AAL5SNAP, AAL5MUX IP, or AAL5MUX PPP.[1]
Step 9	**tx-ring-limit** *number*	Configures the size of the PVC transmit queue. The default setting is 6.
Step 10	**no shutdown**	Enables the ATM interface.
Step 11	**exit**	Exits 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, see the Cisco IOS Release 12.2 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 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

To configure parameters to control access to the router, use the following table, beginning in global configuration mode.

	Command	Purpose
Step 1	**line console 0**	Enters line configuration mode, and specify the console terminal line.
Step 2	**password** *password*	Specifies a unique password on the line.
Step 3	**login**	Enables password checking at terminal session login.
Step 4	**exec-timeout 10 0**	Sets the interval that EXEC command interpreter waits until user input is detected. Exec-timeout 10 0 is the default.
Step 5	**line vty 0 4**	Specifies a virtual terminal for remote console access.
Step 6	**password** *password*	Specifies a unique password on the line.
Step 7	**login**	Enables password checking at virtual terminal session login.
Step 8	**end**	Exits line configuration mode, and return to privileged EXEC mode.

For complete information on the command line commands, see the Cisco IOS Release 12.2 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 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.

To configure bridging, use the following table, beginning in global configuration mode.

	Command	Purpose
Step 1	**no ip routing**	Disables IP routing.
Step 2	**bridge** *number* **protocol** *protocol*	Specifies the bridge protocol to define the type of Spanning-Tree Protocol (STP).
Step 3	**interface ethernet 0**	Enters configuration mode for the Ethernet interface.
Step 4	**bridge-group** *number*	Specifies the bridge-group number to which the Ethernet interface belongs.
Step 5	**no shutdown**	Enables the Ethernet interface.
Step 6	**exit**	Exits configuration mode for the Ethernet interface and the router.
Step 7	**interface ATM 0**	Enters configuration mode for the ATM interface.
Step 8	**dsl equipment-type** {**co** | **cpe**}	Configures the DSL equipment type, if applicable.
Step 9	**dsl linerate** {*number* | **auto**}	Specifies the G.SHDSL line rate, if applicable. The range of valid numbers is between 72 and 2312.
Step 10	**dsl operating-mode gshdsl symmetric annex** *annex*	Sets the G.SHDSL operating mode, if applicable, and select the G.991.2 annex.
Step 11	**pvc** *vpi/vci*	Creates an ATM PVC for each end node with which the router communicates.
Step 12	**encapsulation** *type*	Specifies the encapsulation type for the PVC.
Step 13	**bridge-group** *number*	Specifies the bridge-group number to which the ATM interface belongs.
Step 14	**no shutdown**	Enables the ATM interface.
Step 15	**end**	Exits the configuration mode for the ATM interface.

For complete information on the bridging commands, see the Cisco IOS Release 12.2 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 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#show 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.

To configure static routing, use the following table, beginning in global configuration mode.

	Command	Purpose
Step 1	**ip classless**	Sets up a best route for packets destined for networks unknown by the router.
Step 2	**ip route** *network-number mask*	Specifies the static route for the IP packets.
Step 3	**end**	Exits router configuration mode.

For complete information on the static routing commands, see the Cisco IOS Release 12.2 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 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#show 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 (IGRP) to learn routes dynamically. You can configure either one of these routing protocols.

Configuring RIP

To configure RIP routing protocol on the router, use the following table, 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, see the Cisco IOS Release 12.2 documentation set. For more general information on RIP, see 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 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 example shown below.

```
router#show 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 Enhanced IGRP

To configure IP Enhanced IGRP, use the following table, beginning in global configuration mode.

	Command	Purpose
Step 1	**router eigrp** *autonomous-system*	Enters router configuration mode and enable Enhanced IGRP on the router. The autonomous-system number identifies the route to other Enhanced IGRP routers and is used to tag the Enhanced IGRP information.
Step 2	**network** *network-number*	Specifies the network number for each directly connected network.
Step 3	**end**	Exits router configuration mode.

For complete information on the IP Enhanced IGRP commands, see the Cisco IOS Release 12.2 documentation set. For more general information on Enhanced IGRP concepts, see Chapter 1, "Concepts."

Configuration Example

The following configuration shows Enhanced IGRP routing protocol enabled in IP networks 10.0.0.0 and 172.17.0.0. The Enhanced IGRP 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 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 Enhanced IGRP, enter the **show ip route** command and look for Enhanced IGRP routes signified by “D.” You should see a verification output like the example shown below.

```
router#show 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.

To configure static or dynamic inside source translation using NAT, use the following table, beginning in global configuration mode.

	Command	Purpose
Step 1	**ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}	Creates pool of global IP addresses for NAT.
Step 2	**access-list** *access-list-number* **permit** *source* [*source-wildcard*]	Defines a standard access list permitting addresses that need translation.
Step 3	**ip nat inside source list** *access-list-number* **pool** *name*	Enables 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**	Enables static translation of specified inside local address to globally unique IP address. This command is optional.
Step 5	**interface ethernet 0**	Enters configuration mode for Ethernet interface.
Step 6	**ip nat inside**	Establishes Ethernet interface as inside interface.
Step 7	**exit**	Exits configuration mode for Ethernet interface.
Step 8	**interface atm 0**	Enters configuration mode for ATM interface.

	Command	Purpose
Step 9	**dsl equipment-type** {**co** | **cpe**}	Configures the DSL equipment type, if applicable.
Step 10	**dsl linerate** {*number* | **auto**}	Specifies 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*	Sets the G.SHDSL operating mode, if applicable, and select the G.991.2 annex.
Step 12	**ip nat outside**	Establishes ATM interface as outside interface.
Step 13	**exit**	Exits configuration mode for 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, see the Cisco IOS Release 12.2 documentation set. For more 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 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#show 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.

To configure Easy IP (Phase 1), use the following table, beginning in global configuration mode.

	Command	Purpose
Step 1	**access-list** *access-list-number* **permit** *source* [*source-wildcard*]	Defines a standard access list that permits nonregistered IP addresses of hosts.
Step 2	**ip nat inside source list** *access-list-number* **interface** *interface* **overload**	Sets up translation of addresses identified by the access list defined in Step 1.
Step 3	**interface ethernet 0**	Enters configuration mode for Ethernet interface.
Step 4	**ip nat inside**	Establishes the Ethernet interface as inside interface for NAT.
Step 5	**no shutdown**	Enables the Ethernet interface and the configuration changes just made to it.
Step 6	**exit**	Exits configuration mode for Ethernet interface.
Step 7	**interface dialer**	Enters configuration mode for the dialer interface.
Step 8	**ip address negotiated**	Assigns a negotiated IP address to the dialer interface.
Step 9	**ip nat outside**	Establishes the dialer interface as the outside interface for NAT.
Step 10	**dialer pool** *number*	Specifies which dialer pool number you are using.
Step 11	**exit**	Exits the dialer interface.
Step 12	**interface ATM 0**	Enters configuration mode for the ATM interface.

	Command	Purpose
Step 13	**dsl equipment-type** {**co** | **cpe**}	Configures the DSL equipment type, if applicable.
Step 14	**dsl linerate** {*number* | **auto**}	Specifies the G.SHDSL line rate, if applicable. The range of valid numbers is between 72 and 2312.
Step 15	**dsl operating-mode gshdsl symmetric annex** *annex*	Sets the G.SHDSL operating mode, if applicable, and select the G.991.2 annex.
Step 16	**pvc** *vpi/vci*	Creates an ATM PVC for each end node with which the router communicates.
Step 17	**encapsulation aal5mux ppp dialer**	Specifies the encapsulation type for the PVC to be AAL5MUX PPP and point back to the dialer interface.
Step 18	**dialer pool-member** *number*	Specifies which dialer pool-member you are using.
Step 19	**no shutdown**	Enables the interface and configuration changes just made to the ATM interface.
Step 20	**exit**	Exits configuration mode for the ATM interface.

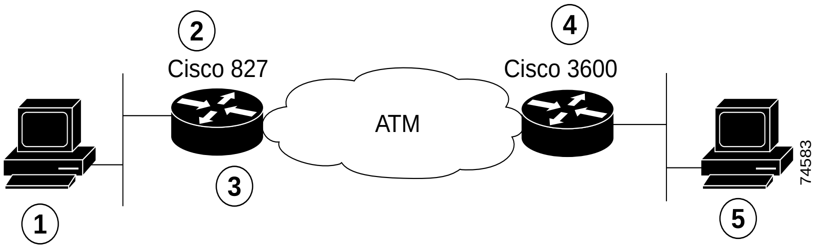
For complete information on the Easy IP commands, see the Cisco IOS Release 12.2 documentation set. For more general information on Easy IP (Phase 1) concepts, see Chapter 1, “Concepts.”

Configuring Easy IP (Phase 2)

This section explains how to configure the Cisco 800 series routers as DHCP servers.

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 3-1.

Figure 3-1 Easy IP (Phase 2) – DHCP Server and Relay



1	DHCP client	**4**	Corporate office
2	Remote office	**5**	DHCP server
3	DHCP relay		

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 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 827 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 12.2
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

To configure the router as a DHCP server, use the following table, beginning in global configuration mode.

	Command	Purpose
Step 1	**ip dhcp pool** *name*	Enters DHCP configuration mode, and create a pool of IP addresses that can be assigned to DHCP clients.
Step 2	**network** *ip-address subnet-mask*	Specifies a range of IP addresses that can be assigned to the DHCP clients.
Step 3	**domain-name** *domain name*	Configures the domain name.
Step 4	**dns-server** *ip-address*	Designates the router as the default router, and specify an IP address.
Step 5	**netbios-name-server** *ip-address*	Configures the netbios name server.
Step 6	**default-router** *ip-address*	Configures the DNS server.
Step 7	**lease** *days hours minutes*	Specifies the duration of the lease.
Step 8	**exit**	Exits DHCP configuration mode.

For more information on the features not used in this configuration, see the *Cisco IOS DHCP Server* feature module. For more general information on DHCP servers, see 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# show 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.

To configure the DHCP relay, use the following table, beginning in global configuration mode.

	Command	Purpose
Step 1	**interface Ethernet 0**	Enters configuration mode for the Ethernet interface.
Step 2	**ip helper-address** *address*	Forwards default UDP broadcasts including IP configuration requests to the DHCP server.
Step 3	**no shutdown**	Enables the Ethernet interface and the configuration changes.
Step 4	**exit**	Exits configuration mode for the Ethernet interface.

For complete information on the DHCP relay commands, see the Cisco IOS Release 12.2 documentation set. For more general information on DHCP relays, see 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 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 a verification output like the example shown below.

```
router#show 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 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+, you must perform the following tasks:

Step 1 Use the **aaa new-model** global configuration command to enable AAA. AAA must be configured if you plan to use TACACS+.

Step 2 Use the **tacacs-server host** command to specify the IP address of one or more TACACS+ daemons.

Step 3 Use the **tacacs-server key** command to 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.

Step 4 Use the **aaa authentication** global configuration command to define the method lists that use TACACS+ for authentication.

Step 5 Use line and interface commands to apply the defined method lists to various interfaces.

You may need to perform other configuration steps if you need to enable accounting for TACACS+ connections. For instructions on configuring TACACS+, see the *Security Configuration Guide*.

Configuring an Extended Access List

To include one or more extended access lists in your router configuration, you can use the following commands, beginning in global configuration mode.

	Command	Purpose
Step 1	**access-list 100 permit tcp any ip** *ip address-mask* **established**	Permits any host on the network to access any Internet server.
Step 2	**access-list 100 deny ip** *ip address-mask* **any**	Denies any Internet host from spoofing any host on the network.
Step 3	**access-list 100 permit tcp host** *ip address-mask*	Permits Internet DNS server to send TCP replies to any host on the network.
Step 4	**access-list 100 permit udp host** *ip address-mask*	Permits Internet DNS server to send UDP replies to any host on the network.
Step 5	**access-list 100 permit tcp any host** *ip address*	Permits SMTP mail server to access any Internet server.
Step 6	**access-list 100 permit tcp any host** *ip address*	Permits web server to access any Internet server.
Step 7	**access-list 100 permit tcp any host** *ip address*	Permits FTP server to access any Internet server.
Step 8	**access-list 100 deny tcp any** *ip address-mask*	Restricts any Internet host from making a Telnet connection to any host on the network.
Step 9	**interface atm 0**	Enters configuration mode for the ATM interface.
Step 10	**dsl equipment-type** *co/cpe*	Configures the DSL equipment type, if applicable.

	Command	Purpose
Step 11	**dsl linerate** *number/auto*	Specifies 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*	Sets the G.SHDSL operating mode, if applicable, and select the G.991.2 annex.
Step 13	**ip access-group 100 in**	Activates access list 100.
Step 14	**no shutdown**	Enables interface and configuration changes made to the interface.
Step 15	**exit**	Exits configuration mode for the ATM interface.

For more complete information on the extended access list commands, see the Cisco IOS Release 12.2 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 requirements for voice QoS are:

- 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 Cisco IOS to provide priority queuing, using Class Based Weighted Fair Queuing (CBWFQ) to prioritize voice traffic and 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, see the Cisco IOS documentation set. For more general information on QoS concepts, see Chapter 1, “Concepts.”

Configuring a Single PVC Environment

In the single PVC environment, the traffic relies on Cisco IOS to provide priority queuing (using CBWFQ). The tasks to configure a single PVC environment are:

- 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. So you need to ensure that the data IP packets do not have the same IP precedence as that of the voice packets.

To configure real-time voice traffic precedence over other IP network traffic, use the following table, beginning in global configuration mode.

	Command	Purpose
Step 1	**dial-peer voice** *number* **voip**	Enters the dial peer configuration mode to configure a VoIP dial peer.
Step 2	**destination-pattern** *number*	Sets a destination pattern.
Step 3	**session target** {**ipv4**:*destination-address*}	Specifies a destination IP address for the dial peer.
Step 4	**ip precedence** *number*	Selects a precedence level for the voice traffic associated with that dial peer.
Step 5	**exit**	Exits 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

To create a policy map and associate a priority queue to the voice class, use the following table, beginning in global configuration mode.

	Command	Purpose
Step 1	**access-list 101 permit ip** *any any precedence 5*	Configures an access list to match voice packets.
Step 2	**class-map** *voice*	Configures a voice class.
Step 3	**match access-group 101**	Associates the voice class with the access list.

Configure a Policy Map and Specify Voice Queuing

Follow the steps below to configure a policy map and to specify voice queuing, beginning in global configuration mode.

	Command	Purpose
Step 1	**policy map** ***name***	Configures a policy map[1].
Step 2	**class** ***voice***	Specifies the class for queuing.
Step 3	**priority** ***number***	Specifies 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

To associate the policy map to the ATM PVC and decrease the MTU of the ATM interface so that large data packets are fragmented, use the following table, beginning in global configuration mode.

	Command	Purpose
Step 1	**policy map** *name*	Configures a policy map[1].
Step 2	**class** *voice*	Specifies the class for queuing.
Step 3	**priority** *bandwidth*	Specifies the priority for queuing.
Step 4	**exit**	Exits 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

To associate the policy map to the ATM PVC and decrease the MTU, use the following table, beginning in global configuration mode. It is recommended that *300* be 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	Purpose
Step 1	**interface ATM 0**	Enters configuration mode for the ATM interface.
Step 2	**ip address** *ip-address mask*	Sets the IP address and subnet mask for the ATM interface.
Step 3	**pvc** *vpi/vci*	Creates an ATM PVC for each end node with which the router communicates.
Step 4	**encapsulation** *protocol*	Specifies the encapsulation type for the PVC. Encapsulations can be specified as AAL5SNAP or AAL5MUX PPP.
Step 5	**service policy out** *name*	Associates the service policy name.

	Command	Purpose
Step 6	**vbr-rt** *pcr scr bs*	Specifies the service class.
Step 7	**exit**	Exits configuration mode for the ATM PVC.
Step 8	**mtu** *number*	Specifies the MTU for the ATM interface.
Step 9	**no shutdown**	Enables the ATM interface.
Step 10	**exit**	Exits 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
!
```

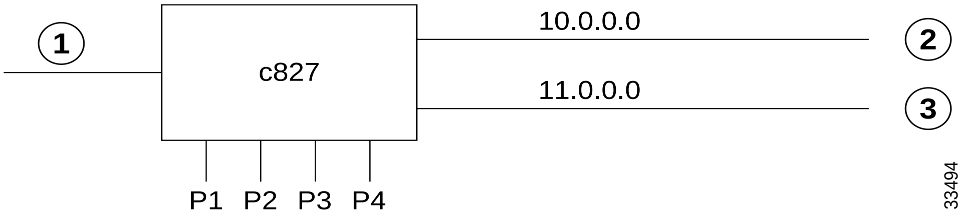
Configuring a Multiple PVC Environment

In a multiple PVC environment, the traffic relies on the ATM interface to provide priority queuing for voice and fragmentation and interleaving. The following figures show the configurations that you can use.

Voice and Data on Different Subnets

Figure 3-2 shows voice and data packets on different subnets. You can have all voice traffic on an ATM PVC with a VBR-RT service class while the data traffic is transported on an ATM PVC with a UBR service class.

Figure 3-2 Voice and Data on Different Subnets



1	Ethernet 0
2	PVC 1/40 VBR (RT), Voice
3	PVC 8/35 UBR, Data

Configuring the ATM Interface and Subinterfaces

Use this table to configure the ATM interface and subinterfaces, beginning in global configuration mode.

	Command	Purpose
Step 1	**interface ATM 0.1 point-to-point**	Specifies the ATM0.1 subinterface.
Step 2	**ip address** *ip-address mask*	Sets the IP address and subnet mask for the ATM0.1 subinterface.
Step 3	**pvc** *vpi/vci*	Creates an ATM PVC for each end node with which the router communicates.
Step 4	**encapsulation** *type*	Specifies the encapsulation type for the PVC.
Step 5	**protocol ip** *address* **broadcast**	Sets the protocol broadcast for the IP address.
Step 6	**interface ATM 0.2 point-to-point**	Specifies the ATM0.2 subinterface.
Step 7	**ip address** *ip-address mask*	Sets the IP address and subnet mask for the ATM0.2 subinterface.
Step 8	**pvc** *vpi/vci*	Creates an ATM PVC for each end node with which the router communicates.
Step 9	**encapsulation** *type*	Specifies the encapsulation type for the PVC.
Step 10	**protocol ip** *address* **broadcast**	Sets the protocol broadcast for the IP address.
Step 11	**exit**	Exits 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.

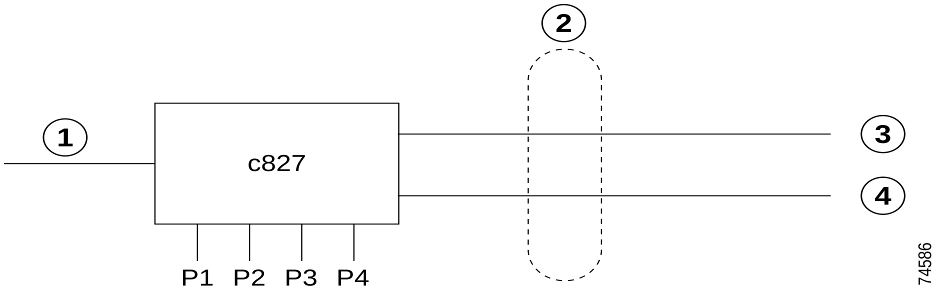
You do not need to enter the commands marked "default." These commands appear automatically in the configuration file generated when you use the **show running-config** command.

```
!
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 3-3 shows 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 the voice packets but not to the data packets ensures that the two types of traffic are separated onto two PVCs.

Figure 3-3 Voice and Data on the Same Subnet with Virtual Circuit Bundling



1	Ethernet 0	**3**	PVC Bundle 1/40 BVR (RT), Voice
2	Bundle	**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 packet

Configuring the ATM Interface

Use the following table to configure the ATM interface, beginning in global configuration mode.

	Command	Purpose
Step 1	**interface ATM 0**	Enters configuration mode for the ATM interface.
Step 2	**dsl equipment-type** *co/cpe*	Configures the DSL equipment type.
Step 3	**dsl linerate** *number/auto*	Specifies the G.SHDSL line rate. The range of valid numbers is between 72 and 2312.
Step 4	**dsl operating-mode gshdsl symmetric annex** *annex*	Sets the G.SHDSL operating mode, and selects the G.991.2 annex.
Step 5	**ip address** *ip-address mask*	Sets the IP address and subnet mask for the ATM interface.
Step 6	**bundle** *name*	Specifies a bundle name.
Step 7	**encapsulation** *type*	Specifies the encapsulation type for the voice bundle PVC.
Step 8	**protocol ip** *ip-address* **broadcast**	Sets the protocol broadcast for the IP address.
Step 9	**pvc-bundle** *name vpi/vci*	Creates a PVC for the voice bundle.
Step 10	**vbr-rt** *pcr scr bs*	Sets the service class for the voice bundle.[1]
Step 11	**ip precedence** *number*	Selects an IP precedence level specific to the voice bundle that you created.
Step 12	**pvc-bundle** *name vpi/vci*	Creates a PVC for the data bundle.
Step 13	**ubr** *pcr*	Sets the service class for the data[2] bundle.
Step 14	**precedence** *other*	Sets the IP precedence level *other* to the data bundle that you created.
Step 15	**exit**	Exits 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

To configure real-time voice traffic precedence over other IP network traffic, use the following table, beginning in global configuration mode.

	Command	Purpose
Step 1	**dial-peer voice** *number* **voip**	Enters the dial peer configuration mode to configure a VoIP dial peer.
Step 2	**destination-pattern** *number*	Sets a destination pattern.
Step 3	**session target** {**ipv4**:*destination-address*}	Specifies a destination IP address for the dial peer.
Step 4	**precedence** *number*	Selects 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 of 5 be 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 two types of 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 Multilink PPP Fragmentation and Interleaving

You should configure multilink PPP fragmentation if you have point-to-point connection using PPP encapsulation or links slower than 2 Mbps in your network.

PPP support for interleaving can be configured on dialer or PRI interfaces.

To configure multilink PPP and interleaving on a dialer interface, use the following table, beginning in global configuration mode.

	Command	Purpose
Step 1	**interface dialer**	Enters configuration mode for the dialer interface.
Step 2	**ppp multilink**	Enables multilink PPP for the dialer interface.
Step 3	**bandwidth** *n*	Specifies 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.

	Command	Purpose
Step 4	**ppp multilink interleave**	Enables interleaving for RTP packets among the fragments of larger packets on a multilink PPP bundle.
Step 5	**ppp multilink fragment-delay** *milliseconds*	Configures a maximum fragment delay of 20 ms. This command is optional.
Step 6	**ip rtp reserve** *lowest-UDP-port range-of-ports* [*maximum-bandwidth*]	Reserves a special queue for real-time packet flows to specified destination UDP ports, allowing real-time traffic to have higher priority than other flows. This only applies if you have **not** configured RSVP.
Step 7	**exit**	Exits configuration mode for the dialer interface.

Note You can use the **ip rtp reserve** command instead of configuring RSVP. If you configure RSVP, this command is not required.

For complete information on the PPP fragmentation and interleaving commands, see the *Dial Solutions Configuration Guide* for Cisco IOS Release 12.2. For more 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 a higher priority than other IP data traffic. The **ip precedence** command should also be used if RSVP is not enabled and you would like to give voice packets a priority over other IP data traffic. IP Precedence scales better than RSVP, but it provides no admission control.

To configure real-time voice traffic precedence over other IP network traffic, use the following table, beginning in global configuration mode.

	Command	Purpose
Step 1	**configure terminal**	Enters configuration mode.
Step 2	**dial-peer voice** *number* **voip**	Enters the dial peer configuration mode to configure a VoIP dial peer.
Step 3	**destination-pattern** *number*	Sets a destination pattern.
Step 4	**ip precedence** *number*	Selects 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, see the Cisco IOS Release 12.2 documentation set. For more 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 by the Cisco 827 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 generated when you use the **show running-config** command.

```
!
access-list 101 permit
route-map data permit 10
set ip precedence routing
!
```

Configuring RSVP

To minimally configure RSVP for voice traffic, you must enable RSVP on each interface where priority needs to be set. The RSVP feature applies to a single-PVC network only.

By default, RSVP is disabled so that it is backwards compatible with systems that do not implement RSVP. To enable RSVP for IP on an interface, use the following interface configuration command:

```
Router(config-if)# ip rsvp bandwidth [interface-kbps] [single-flow-kbps]
```

This command starts RSVP and sets the bandwidth and single-flow limits. The default maximum bandwidth is up to 75 percent of the bandwidth available on the interface. By default, a flow can reserve up to the entire reservable bandwidth.

On subinterfaces, RSVP applies to the more restrictive of the available bandwidths of the physical interface and the subinterface.

After enabling RSVP, you must also use the **req-qos** dial-peer configuration command to request an RSVP session on each VoIP dial peer. Otherwise, no bandwidth is reserved for voice traffic.

To request an RSVP session on each VoIP dial peer, use the following table, beginning in global configuration mode:

	Command	Purpose
Step 1	**configure dial-peer**	Enters configuration mode for the dial peer.
Step 2	**dial-peer voice** *number* **voip**	Assigns the dial peer voice number to configure a VoIP dial peer.
Step 3	**req-qos controlled load**	Requests an RSVP session for each dial peer.

For more information about configuring RSVP, see the "Configuring RSVP" chapter of the *Network Protocols Configuration Guide, Part 1,* for Cisco IOS Release 12.2. For more general information on RSVP commands, see Chapter 1, "Concepts."

Configuration Example

This configuration shows two voice dial peers (number 211 and 212) being configured for RSVP.

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.

```
!
dial-peer voice 211 voip
req-qos controlled-load
!
dial-peer voice 212 voip
       req-qos controlled-load
!
```

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 Cisco IOS, please go to the following URL:

http://www.cisco.com/en/US/tech/tk801/tk133/technologies_tech_note09186a008009457d.shtml

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	Purpose
Step 1	**ip multicast-routing**	Enables IP multicast forwarding.
Step 2	**ip pim rp-address** *address*	Configures the Protocol Independent Multicast (PIM) Rendezvous Point (RP) address.
Step 3	**interface ethernet 0**	Enters Ethernet 0 interface configuration mode.
Step 4	**ip address** *ip-address subnet-mask*	Configures an IP address and subnet mask for the Ethernet 0 interface.
Step 5	**ip pim** { **sparse** |**dense** }**-mode**	Configures the Ethernet 0 interface for PIM sparse mode or PIM dense mode.
Step 6	**interface Ethernet 1**	Enters Ethernet 1 configuration mode.
Step 7	**ip address** {*ip-address subnet-mask* ***negotiated***}	Specifies an IP address and subnet mask for the dialer interface, or indicates that the IP address is to be negotiated.
Step 8	**ip pim** {*sparse* | *dense*} **-mode**	Configures the dialer interface for PIM sparse mode or PIM dense mode.

	Command	Purpose
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**	Exits router configuration mode.
Step 11	**interface loopback 0**	Enters loopback interface configuration mode.
Step 12	**ip address** *ip-address subnet-mask*	Configures an IP address and subnet mask for the loopback 0 interface.
Step 13	**ip pim sparse-mode**	Configures the loopback interface for PIM sparse mode or PIM dense mode.
Step 14	**ip igmp helper-address udl ethernet 0**	Enters IGMP helper-address unidirectional link to Ethernet 0
Step 15	**ip igmp proxy-service**	Enables 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.

Configuring Internet Protocol Parameters

Follow the steps below to configure IP parameters, starting in global configuration mode.

	Command	Purpose
Step 1	**ip subnet-zero**	Configures the router to recognize the zero subnet range as the valid range of addresses.
Step 2	**no ip finger**	Blocks incoming IP finger packets.
Step 3	**no ip domain-lookup**	Disables the router from interpreting unfamiliar words (typographical errors) as host names entered during a console session.
Step 4	**ip classless**	Follows 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 endpoint.

Configuring IPSec

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

	Command	Purpose
Step 1	**crypto isakmp policy 10**	Defines an Internet Key Exchange (IKE) policy, and assigns the policy a priority. This command places the router in IKE policy configuration mode.
Step 2	**hash md5**	Specifies the MD5 hash algorithm for the policy.
Step 3	**authentication pre-share**	Specifies pre-share key as the authentication method.
Step 4	**exit**	Exits IKE policy configuration mode.
Step 5	**crypto isakmp key** *name* **address** *ip-address*	Configures a pre-shared key and static IP address for each VPN client.
Step 6	**crypto ipsec transform-set** *name* **esp-des esp-md5-hmac**	Defines a combination of security associations to occur during IPSec negotiations.
Step 7	**crypto map** *name* **local-address ethernet 1**	Creates a crypto map, and specifies and names an identifying interface to be used by the crypto map for IPSec traffic.

	Command	Purpose
Step 8	**crypto map** *name seq-num* **ipsec-isakmp**	Enters crypto map configuration mode, and creates a crypto map entry in IPSec ISAKMP mode.
Step 9	**set peer** *ip-address*	Identifies the remote IPSec peer.
Step 10	**set transform-set** *name*	Specifies the transform set to be used.
Step 11	**match address** *access-list-id*	Specifies an extended access list for the crypto map entry.
Step 12	**exit**	Exits 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	Purpose
Step 1	**interface tunnel 0**	Configures the tunnel 0 interface.
Step 2	**ip address** *ip-address subnet-mask*	Sets the IP address and subnet mask for the tunnel 0 interface.
Step 3	**tunnel source ethernet 1**	Specifies the Ethernet 1 interface as the tunnel source.
Step 4	**tunnel destination** *default-gateway-ip-address*	Specifies the default gateway as the tunnel destination.
Step 5	**crypto map** *name*	Associates a configured crypto map to the tunnel 0 interface.
Step 6	**exit**	Exits 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	Purpose
Step 1	**interface ethernet 0**	Configures the Ethernet 0 interface.
Step 2	**ip address** *ip-address subnet-mask*	Sets the IP address and subnet mask for the Ethernet 0 interface.
Step 3	**exit**	Exits the Ethernet 0 interface configuration.
Step 4	**interface ethernet 1**	Configures the Ethernet 1 interface.
Step 5	**ip address** *ip-address subnet-mask*	Sets the IP address and subnet mask for the Ethernet 1 interface.

	Command	Purpose
Step 6	**crypto map** *name*	Associates a crypto map with the Ethernet 1 interface.
Step 7	**end**	Exits router configuration mode.

Configuring Static Routes

Follow the steps below to configure static routes, starting in global configuration mode.

	Command	Purpose
Step 1	**ip route** *default-gateway-ip-address mask* **ethernet 1**	Creates a static route for the Ethernet 1 interface.
Step 2	**ip route** *default-gateway-ip-address mask* **tunnel 0**	Creates a static route for the tunnel 0 interface.
Step 3	**ip route** *default-gateway-ip-address mask gateway-of-last-resort*	Creates a static route to the gateway of last resort.
Step 4	**end**	Exits 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, see 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 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	Purpose
Step 1	**interface dialer**	Enters configuration mode for the dialer interface.
Step 2	**ppp multilink**	Enables multilink PPP for the dialer interface.
Step 3	**bandwidth** *n*	Specifies 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**	Enables interleaving for RTP packets among the fragments of larger packets on a multilink PPP bundle.
Step 5	**ppp multilink fragment-delay** *milliseconds*	Configures a maximum fragment delay of 20 ms. This command is optional.
Step 6	**ip rtp reserve** *lowest-UDP-port range-of-ports* [*maximum-bandwidth*]	Reserves 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**	Exits configuration mode for the dialer interface.

For complete information on the PPP fragmentation and interleaving commands, see 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	Purpose
Step 1	**configure terminal**	Enters configuration mode.
Step 2	**dial-peer voice** *number* **voip**	Enters the dial peer configuration mode to configure a VoIP dial peer.
Step 3	**destination-pattern** *number*	Sets a destination pattern.
Step 4	**ip precedence** *number*	Selects 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, see the Cisco IOS Release 12.2 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

The Cisco 827 routers support voice using the H.323 signaling protocol.

- H.323
- SGCP

The default signaling protocol is H.323 signaling standard.

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

To configure the POTS dial peers, use the following table, beginning in global configuration mode.

	Command	Purpose
Step 1	**dial-peer voice** *number* **POTS**	Enters configuration mode for the dial peer.
Step 2	**destination-pattern** *string*	Defines the destination telephone number associated with the VoIP dial peer.
Step 3	**port** *number*	Specifies the port number.

Configuring Voice Dial Peers for H.323 Signaling

Follow the steps below to configure voice dial peers for H.323 signaling, beginning in global configuration mode.

	Command	Purpose
Step 1	**dial-peer voice** *number* **VoIP**	Enters configuration mode for the dial peer.
Step 2	**destination-pattern** *string*	Defines the destination telephone number associated with each VoIP dial peer.

	Command	Purpose
Step 3	**codec** *string*	Specifies a codec if you are not using the default codec of g.729.
Step 4	**session target** {**ipv4**:*destination-address*}	Specifies 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, if you are overseas, you may need to do the following voice port configuration, beginning in global configuration mode.

	Command	Purpose
Step 1	**configure dial-peer**	Enters configuration mode for the dial peer.
Step 2	**voice-port** *port*	Identifies the voice port you want to configure and enters the voice port configuration mode.
Step 3	**cptone** *country*	Selects the appropriate voice call progress tone for this interface. The default country for this command is **us**.
Step 4	**ring frequency (25 \ 50)**	Selects 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*	Attaches descriptive text about this voice port connection.
Step 6	**comfort-noise**	If voice activity detection (VAD) is activated, this command specifies that background noise is generated.
Step 7	**impedance**	Specifies 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, see the Cisco IOS Release 12.2 documentation set. For more 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, see 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 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 Routers Configuration Examples

The following examples are 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. These commands appear automatically in the configuration file generated when you use the **show running-config** command.

```
Current configuration:
!
version 12.2
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 generated when you use the **show running-config** command.

```
Current configuration:
!
version 12.2
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 12.2
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
```

Advanced Router Configuration

This chapter includes advanced configuration procedures.

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 2, "Network Scenarios." For basic router configuration topics, see Chapter 3, "Basic Router Configuration."

This chapter contains the following sections:

- Configuring DSL Commands, page 4-41
- Configuring FTP Client, page 4-45

Each section includes a configuration example and verification steps, where available.

Configuring PPP over Ethernet Support

The following sections describe how to configure PPP over Ethernet support:

- Configuring PPPoE Client Support
- Configuring TCP Maximum Segment Size for PPP over Ethernet

Configuring PPPoE Client Support

PPPoE is supported on the following Cisco routers:

- Cisco 826 and Cisco 836
- Cisco 827, Cisco 827H, Cisco 827-4V, and Cisco 837
- Cisco 828
- Cisco 831
- Cisco SOHO 77, Cisco SOHO 77H, Cisco SOHO 78, Cisco SOHO 96, and Cisco SOHO 97

This feature supports the PPP over Ethernet (PPPoE) client on an ATM permanent virtual circuit (PVC). Only one PPPoE client on a single ATM PVC is supported.

A PPPoE session is initiated on the client side by the network described above. If the session has a timeout or is disconnected, the PPPoE client immediately attempts to reestablish the session.

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. Configure authentication for your network by entering the **ppp authentication** protocol command. This step is optional.

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.

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

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 PPP over Ethernet

If a Cisco router terminates the PPP over Ethernet (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.

Network address translation (NAT) must be configured for the **ip tcp adjust-mss** command to work.

This feature is not supported on Cisco SOHO 76 routers.

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 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 826 and Cisco 836
- Cisco 827, Cisco 827H, Cisco 827-4V, and Cisco 837
- Cisco SOHO 77, Cisco SOHO 77H, Cisco SOHO 78, Cisco 96, and Cisco 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.

Network address translation (NAT) must be configured in order for the **ip tcp adjust-mss** command to work.

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 routers:

- Cisco 826 and Cisco 836
- Cisco 827, Cisco 827H, Cisco 827-4V, Cisco 831, and Cisco 837
- Cisco 828
- Cisco SOHO 77, Cisco SOHO 77H, Cisco SOHO 78, Cisco SOHO 91, Cisco SOHO 96, and Cisco SOHO 97

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 LLQ

Follow these steps 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 the 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.

Note Attach the service policy to the dialer interface only when LFI is used. Else, the service policy must be attached under the PVC itself.

Configuring LFI

Follow these steps 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 permanent virtual circuits (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 Cisco 831 router.

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, see 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 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 831-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 Cisco 836
- Cisco 827, Cisco 827H, Cisco 827-4V, and Cisco 837
- Cisco 828
- Cisco SOHO 77, Cisco SOHO 77H, Cisco SOHO 78, Cisco SOHO 96, and Cisco SOHO 97

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

This feature is supported on the following Cisco routers:

- Cisco 826 and Cisco 836
- Cisco 827, Cisco 827H, Cisco 827-4V, and Cisco 837
- Cisco 828
- Cisco 831
- Cisco SOHO 77, Cisco SOHO 77H, Cisco SOHO 78, Cisco SOHO 91, Cisco SOHO 96, and Cisco SOHO 97

Before Cisco IOS Release 12.1(5), the only way to configure the DHCP options on the Cisco IOS DHCP server was through the command-line interface (CLI). However, you may not want to configure the same DHCP options on multiple DHCP servers if you can, instead, configure a remote master DHCP server located on the corporate backbone. In this case, all the local DHCP servers will have the same DHCP options as those configured on the remote DHCP server.

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) server, the Windows Information Name Server (WINS), or the NetB Cisco IOS Name Service (NBNS), and the server IP address information within a Cisco IOS DHCP server pool.

Follow these steps 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 configuration of the DHCP server import on the Cisco router:

```
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 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 DHCP proxy client configuration:

```
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 configuration on the remote DHCP server:

```
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 826 and Cisco 836
- Cisco 827, Cisco 827H, Cisco 827-4V, Cisco 831, and Cisco 837
- Cisco 828
- Cisco SOHO 77, Cisco SOHO 77H, Cisco SOHO 78, Cisco SOHO 91, Cisco SOHO 96, and Cisco SOHO 97

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.

The IPCP feature 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 support is no longer 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 these steps to configure the Cisco router (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 IPCP configuration on the Cisco router (CPE):

```
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 IPCP configuration on the remote server:

```
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 IPCP configuration on the RADIUS server (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 826 and Cisco 836
- Cisco 827, Cisco 827H, Cisco 827-4V, Cisco 831, and Cisco 837
- Cisco 828
- Cisco SOHO 77, Cisco SOHO 77H, Cisco SOHO 78, Cisco SOHO 96, and Cisco SOHO 97

The Service Assurance Agent (SAA) is an agent that monitors network performance by measuring key factors such as response time, availability, jitter, connect time, throughput, and packet loss.

The SA agent is a new name and an enhancement for the Response Time Reporter (RTR) feature introduced in Cisco IOS Release 11.2.

For configuration information on this command, see the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_c/fcprt3/fcd301d.htm#xtocid135130

Configuring Secure Shell

Secure Shell (SSH) is supported on the following Cisco routers:

- Cisco 826 and 836
- Cisco 827, 827H, 827-4V, 831, and 837
- Cisco 828
- Cisco SOHO 91, SOHO 96, and SOHO 97

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.

For configuration information on this command, see the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s5/sshv1.htm

Configuring IP Named Access Lists

IP named access lists are supported on the following Cisco routers:

- Cisco 826 and Cisco 836
- Cisco 827, Cisco 827H, Cisco 827-4V, Cisco 831, and Cisco 837
- Cisco 828
- Cisco SOHO 77, Cisco SOHO 77H, Cisco SOHO 78, Cisco SOHO 96, and Cisco SOHO 97

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, see the following URL:

http://cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt1/1cdip.htm#xtocid2299616

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

Use the following procedure to configure a voice port to support caller ID, international cadence, impedance, and ring frequency, starting in global configuration mode:

Step 1 Enter the **voice-port** *number* command to enter voice-port configuration mode.

Step 2 Enter the **cptone** *country-code* command to specify settings for call-progress tone, ring cadence, line impedance, and ring frequency.

Step 3 Enter one of the following commands to enable caller ID:

- Enter the **caller-id enable** command to enable caller ID support.
- Enter the **caller-id alerting** *alerting-method* command to enable caller ID support and to specify the alerting method.

Step 4 Enter the **caller-id block** command to request blocking of the display of caller ID information at the far end of the call.

Step 5 Enter **end** to 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.

cptone Command

Use the voice-port configuration mode **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
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

ring cadence Command

To specify the ring cadence for a Foreign Exchange Station (FXS) voice port, use the **ring cadence** command in voice-port configuration mode. 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	.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
pattern11	0.4 second on, 0.2 second off, then 0.4 second on, 2 seconds off
pattern12	0.4 second on, 0.2 second off, then 0.4 second on, 2.6 seconds off

ring frequency Command

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.

impedance Command

To specify the terminating impedance of a voice port interface, use the **impedance** command in voice-port configuration mode. 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.

Configuring International Caller ID

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.

caller-id enable Command

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.

caller-id alerting Command

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. 1–If your telephone service provider specifies it, use this setting to provide caller ID alerting (display) after the first ring at the receiving station. 2–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.

caller-id block Command

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 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 826 and Cisco 836
- Cisco 827, Cisco 827H, Cisco 827-4V, Cisco 831, and Cisco 837

- Cisco 828
- Cisco SOHO 77, Cisco SOHO 78, Cisco SOHO 96, and Cisco SOHO 97

Cisco IOS Release 12.2(2)XI NAT supports IP Security (IPSec) 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 831, Cisco 836, and Cisco 837
- Cisco SOHO 91, Cisco SOHO 96, and Cisco 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

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 c836-1
!
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 these steps to configure ATM Forum Profile 9 support for a voice port, beginning in global configuration mode.

Step 1 Enter the **voice class permanent 1** command to configure a voice class.

Step 2 Enter the **signal timing oos timeout disabled** command to disable the assertion of the receive Out-of-Service (OOS) pattern to the PBX when signaling packets are lost.

Step 3 Enter **exit** to exit voice class configuration mode.

Step 4 Enter **voice service voatm** to enter voice service configuration mode.

Step 5 Enter the **session protocol aal2** command.

Step 6 Enter **mode bles** to indicate that VOATM is to be used in broadband loop emulation service (BLES) mode.

Step 7 Enter **exit** to leave session protocol mode, and then enter **exit** again to leave voice service configuration mode.

Step 8 Enter **interface atm0** to enter ATM 0 interface configuration mode.

Step 9 Enter **pvc** *vpi vci* to specify the virtual path identifier and the virtual channel identifier of the PVC.

Step 10 Enter **vbr-rt** *pcr acr bcs* to 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.

Note One phone line requires a minimum setting of 78 kbps for both PCR and ACR values.

Step 11 Enter **encapsulation aal2** to specify that ATM adaptation layer 2 type encapsulation be used.

Step 12 Enter **no atm cell-clumping-disable** to ensure that sufficient bandwidth is allocated for data packets when voice calls are in progress.

Step 13 Enter **exit** to leave ATM 0 interface configuration mode.

Step 14 Enter the **dial-peer voice** *tag* **voatm** command. This command places the router in dial-peer voice configuration mode.

Step 15 Enter the **session protocol aal2-trunk** command.

Step 16 Enter the **session target atm0 pvc** *vpi/vci* **cid** *cid* command.

This command has the following parameters:

- *vpi*—Virtual path identifier
- *vci*—Virtual channel identifier
- *cid*—AAL2 channel identifier

Step 17 To specify which codec profile the voice dial peer will use, enter one of these **codec aal2 profile** commands, as appropriate:

- Enter **codec aal2-profile atmf 9 g711alaw** to specify that only G.711 a-law be used.
- Enter **codec aal2-profile atmf 9 g711ulaw** to specify that only G.711 mu-law be used.

Step 18 Enter the **destination-pattern** *destination string* command. The *destination string* is the phone number in E.164 format that must match the destination string configured for the voice-port in order to associate a dial-peer with a voice port.

Step 19 Enter the **voice-class permanent 1** command to associate this dial peer with the configured voice class.

Step 20 Enter **no vad** to specify no voice activity detection (VAD).

Step 21 Enter **exit** to leave dial peer voice configuration mode.

Step 22 Enter the **voice port** *#* command to enter voice port configuration mode.

Step 23 Enter the **connection trunk** *destination-pattern* command. The destination pattern must match the *destination-string* configured for the dial peer.

Step 24 Enter the **playout-delay mode fixed no-timestamps** command. This command causes the AAL2 packet to be played at a fixed rate, and the timestamps carried in the packet to be ignored.

Step 25 Enter **end** to exit router configuration mode.

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 4 phone lines, although only 2 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 Cisco 836
- Cisco 827, Cisco 827H, and Cisco 837
- Cisco SOHO 77, Cisco SOHO 96, and Cisco 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.

oam-pvc manage cc Command

The **oam-pvc manage cc** command configures continuity checking on a PVC. Use the **no** form of this command to disable continuity checking on the segment.

```
oam-pvc manage cc segment direction [ source | sink | both ]
no oam-pvc manage cc segment direction [ source | sink | both ]
```

Syntax Description

segment direction specifies the CC cell transmission direction.

source	The router is to act as the source of CC cells.
sink	The router is to act as the sink, or destination, for transmitted CC cells.
both	The router is to act as both source and sink.

Default

The default segment direction is sink.

Command Mode

PVC configuration mode.

Message Guidelines

Using **no oam-pvc manage cc** deactivates continuity checking regardless of the direction in which it is being performed, and regardless of which router initiated continuity checking.

Configuration Examples

The following configuration 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 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 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 deactivates segment CC:

```
interface ATM0
 ip address 10.0.0.3 255.255.255.0
 pvc 0/33
    no oam-pvc manage cc
!
end
```

oam retry cc activation-count deactivation-count retry-frequency Command

The **oam retry cc activation-count deactivation-count retry-frequency** command sets the frequency at which CC activation and deactivation requests are sent to the router at the other end of the segment. The **no** form of this command removes these settings.

oam retry cc activation-count *number* **deactivation-count** *number* **retry-frequency** *seconds*
no oam retry cc activation-count *number* **deactivation-count** *number* **retry-frequency** *seconds*

Syntax Description

activation-count	Specifies the maximum number of times the activation message will be sent before receiving an acknowledgement.
deactivation-count	Specifies the maximum number of times the deactivation message will be sent before receiving an acknowledgement.
retry-frequency	Specifies the interval between retries.

Default

No default.

Command Mode

PVC configuration.

Example Configuration

The following configuration 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
```

oam-pvc manage cc deny Command

The **oam-pvc manage cc deny** 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. The **no** form of this command reenables CC support on the VC.

```
oam-pvc manage cc deny
no oam-pvc manage cc deny
```

Default

CC is supported by default.

Command Mode

PVC configuration mode.

Example Configuration

The following configuration denies segment CC:

```
interface ATM0
 ip address 10.0.0.3 255.255.255.0
 pvc 0/33
    oam-pvc manage cc deny
 !
 end
```

debug atm oam cc Command

You see the results of continuity checking by using the **debug atm oam cc** command. The **no** form of this command disables continuity checking debugging.

```
debug atm oam cc interface atm number
no debug atm oam cc interface atm number
```

Syntax Description

number	ATM interface number.

Default

Disabled.

Command Mode

Privileged EXEC.

Example Output

The following example output of the debug **atm oam cc** command records activity beginning with the entry of the **oam-pvc manage cc** command, and ending with the entry of the **no oam-pvc manage cc** command. The ATM 0 interface was specified, and the “both” segment direction was 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.
1	Sink.
VC 1/40	Virtual circuit identifier.
Direction:3	Indication of the direction in which the cells are traveling. 1 indicates local router is sink. 2 indicates local router is source. 3 indicates both routers operate as source and sink.

Configuring RADIUS Support

Remote Authentication Dial-In User Service (RADIUS) is supported on the following Cisco routers:

- Cisco 826 and Cisco 836
- Cisco 827, Cisco 827H, Cisco 827-4V, Cisco 831, and Cisco 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.

Configuring 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 that perform a high level of authentication and that 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.

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 see 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.

Easy VPN Documentation

The release note "Cisco EZVPN Client for the Cisco uBR905/uBR925 Cable Access Routers" contains instructions for configuring the DHCP server pool, the Easy VPN client profile required to implement Easy VPN, contains example configurations for the IPSec server, and descriptions of **commands available to manage Easy Virtual Private Networking**.

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 Ethernet1 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 output of the **show running-config** command follows:

```
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 826 and Cisco 836
- Cisco 827, 827H, Cisco 827-4V, Cisco 831, and Cisco 837
- Cisco 828
- Cisco SOHO 77, Cisco SOHO 77H, Cisco SOHO 78, Cisco SOHO 91, Cisco SOHO 96, and Cisco SOHO 97

The DDR for PPPoE client feature provides flexibility for subscribers whose ISP charges are based on the amount of time they are connected to the network (non-flat-rate services). With the DDR for PPPoE 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 interesting traffic arrives from the LAN interface and 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**]

Syntax Descriptions

dial-pool-number	Create a dial pool.
dial-on-demand	Activate DDR.

Configuring DDR for a PPPoE Client

Complete the following tasks to configure DDR for a PPPoE client, beginning in global configuration mode:

Step 1 Enable vpdn.

- **a.** Enter the global configuration mode **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 Enter the global interface configuration **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 router configuration mode.

Configuring Weighted Fair Queuing

Weighted fair queuing (WFQ) is supported on the following Cisco routers:

- Cisco 826 and Cisco 836
- Cisco 827, Cisco 827H, Cisco 827-4V, Cisco 831, and Cisco 837
- Cisco 828

WFQ enables slow-speed links, such as serial links, to provide fair treatment for all types of traffic. In order to do this, WFQ classifies the traffic into different flows (also known as conversations) based on layer three and layer four information, such as IP addresses and TCP ports. It does this 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.

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 Weighted Fair Queuing

The following procedure shows how to apply WFQ to the ATM interface of a Cisco router.

Step 1 Create a policy map for WFQ.

a. Enter the **policy-map** *map-name* command in global configuration mode 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	Purpose
Step 1	**dsl noise-margin**	Sets the noise margin offset.
Step 2	**max-tone-bits**	Sets the maximum bits per tone limit.
Step 3	**gain-setting rx-offset**	Sets the receive gain offset.
Step 4	**gain-setting tx-offset**	Sets 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
- 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 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 decide 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 following routers:

- Cisco 827, 827H, and 827-4V
- Cisco 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 the **dsl firmware secondary** command is added 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 FTP Client

The File Transfer Protocol (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

Troubleshooting

Use the information in this chapter to help isolate problems you might encounter 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 listed in the "Related Documents" section on page -xiii.) 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, see 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, see 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 10BaseT 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 using pins 3 and 4 — For more information on the G.SHDSL connection, see 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 digital subscriber line access multiplexer (DSLAM). For more information on the G.SHDSL LEDs, see the *Cisco 828 Router and SOHO 78 Router Hardware Installation Guide.*
- That you are using the correct asynchronous transfer mode (ATM) variable path indentifier/variable circuit identifier (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.

Following is example 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 5-1 describes possible command output for the **show interface** command. Each line in the command output example corresponds to a row in this table.

Table 5-1 Show DSL Interface Command Output Description

Output	Description
Equipment Type	• Customer Premise Equipment (CPE), if connected to a DSLAM. • 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.
Requested rate	User-specified bit rate requirement.
Actual rate	The actual bit rate that the transceiver is using.

Table 5-1 Show DSL Interface Command Output Description (continued)

Output	Description
Modem Status	• Handshake, when local transceiver tries to reach the far-end transceiver. • Training; indicates the startup training is in progress. • 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 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 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.
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 whether 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 5-2, Part 1.

```
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 5-2, Part 1 describes possible command output for the **show interface** command. Each line in the command output example corresponds to a row in this table.

Table 5-2, Part 1 show interface Command Output Description

Output	Description
• ATM0 is up, line protocol is up **Other possible messages:** • ATM0 is down, line protocol is down • ATM0 is down, line protocol is down	• The ATM line is up and operating correctly. • The ATM interface has been disabled with the **shutdown** command. • 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 **Other possible messages:** • ATM0.1 is administratively down, line protocol is down • ATM0.1 is down, line protocol is down	• The first ATM subinterface is up and operating correctly. • The ATM subinterface has been disabled with the **shutdown** command. • The ATM subinterface is down, possibly because the ATM line has been disconnected (by the service provider).
• Ethernet0 is up, line protocol is up **Other possible messages:** • Ethernet0 is up, line protocol is down • Ethernet0 is administratively down, line protocol is down	• The Ethernet interface is connected to the network and operating correctly. • The Ethernet interface has been correctly configured and enabled, but the Ethernet cable might be disconnected from the LAN. • The Ethernet interface has been disabled with the shutdown command, and the interface is disconnected.

Table 5-2, Part 1 show interface Command Output Description (continued)

Output	Description
Dialer1 is up, line protocol is up **Another possible message:** Dialer1 is down, line protocol is down	• Dialer1 is up and operating correctly. • 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
```

Following is an output example 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 5-3 describes the fields shown in the command output.

Table 5-3 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 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 5-4 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. 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 Digital Subscriber Line Access Multiplexer (DSLAM) at the telephone company, the modem state is 0x10. If the interface is not communicating with the DSLAM, the modem state is 0x8.

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 5-5 describes the fields shown in the **debug atm packet** command output.

Table 5-5 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.

Table 5-5 debug atm packet Command Output Description (continued)

Field	Description
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).

Software Upgrade Methods

Following are the methods for upgrading software on Cisco 800-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 only be done 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.com for additional information on replacing enable secret passwords.

Changing the Configuration Register

This section describes how 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.

Step 2 Configure the terminal to operate at 9600 baud, 8 data bits, no parity, and 1 stop bit.

Step 3 At the privileged EXEC prompt (*router_name* >), enter the **show version** command to display the existing configuration register value (shown in bold at the bottom of this output example):

```
820-uut2#sh ver
Cisco Internetwork Operating System Software
Cisco 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

This section describes how 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, see the documentation that came with the terminal for instructions on how to send a break.

Step 2 Press **break**. The terminal displays the following prompt:

```
rommon 2>
```

Step 3 Enter **confreg 0x142** to reset the configuration register:

```
rommon 2> confreg 0x142
```

Step 4 Initialize the router by entering the **reset** command:

```
rommon 2> reset
```

The router cycles its power, and the configuration register is set to 0x142. The router uses the boot ROM system image, indicated by the system configuration dialog:

```
--- System Configuration Dialog ---
```

Step 5 Enter **no** in response to the prompts until the following message is displayed:

```
Press RETURN to get started!
```

Step 6 Press **Return**. The following prompt appears:

```
Router>
```

Step 7 Enter the **enable** command to enter enable mode. Configuration changes can be made only in enable mode:

```
Router> enable
```

The prompt changes to the privileged EXEC prompt:

```
Router#
```

Step 8 Enter the **show startup-config** command to display an enable password in the configuration file:

```
Router# show startup-config
```

If you are recovering an enable password, skip the following "Resetting the Password and Saving Your Changes" section, and complete the password recovery process by performing the steps in the "Resetting the Configuration Register Value" section.

If you are recovering an enable secret password, it is not displayed in the **show startup-config** command output. Complete the password-recovery process by performing the steps in the following "Resetting the Password and Saving Your Changes" section.

Resetting the Password and Saving Your Changes

This section discusses how 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 831 router and the 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/warp/public/cc/pd/nemnsw/rtwbto20/prodlit/cwstu_ds.htm

To see CRWS User's Guide, go to:

http://www.cisco.com/univercd/cc/td/doc/clckstrt/crws/ugcrws30.htm

To see the CRWS Troubleshooting Guide, go to:

http://www.cisco.com/univercd/cc/td/doc/clckstrt/crws/tgcrws31.htm

Cisco IOS Basic Skills

Understanding how to use Cisco IOS software will save you 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, go to Chapter 3, "Basic Router Configuration," and Chapter 4, "Advanced Router Configuration."

This chapter describes what you need to know before you begin configuring your router with Cisco IOS software (the software that runs your router).

This chapter contains the following sections:

- Configuring the Router from a PC
- Understanding Command Modes
- Getting Help
- Enable Secret and Enable Passwords
- Entering Global Configuration Mode
- Using Commands
- Saving Configuration Changes

Configuring the Router from a PC

You can configure your router from a connected PC. For information on how to connect the PC, see the documentation listed in the Obtaining Documentation Section.

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 2000, 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, see 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 later in this chapter.

Understanding Command Modes

This section describes the Cisco IOS command mode structure. Each command mode supports specific Cisco IOS commands. For example, you can use the **interface** *type number* command only from global configuration mode.

The following Cisco IOS command modes are hierarchical. When you begin a router session, you are in user EXEC mode.

- User EXEC
- Privileged EXEC
- Global configuration

Table A-2 lists the command modes that are used in this guide, 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, see the Cisco IOS 12.2 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: • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	Enter the **enable** command from user EXEC mode.	`Router#`	To exit to user EXEC mode, enter the **disable** command. To enter global configuration mode, enter the **configure** command.	Use this mode to: • Configure your router operating parameters. • Perform the verification steps shown in this guide. • To prevent unauthorized changes to your router configuration, access to this mode should be protected with a password as described in "Enable Secret and Enable Passwords" later in this chapter.
Global configuration	Enter the **configure** command from privileged EXEC mode.	`Router (config)#`	To exit to privileged EXEC mode, enter the **exit** or **end** command, or press **Ctrl-Z**. To enter interface configuration mode, enter the **interface** command.	Use this mode to configure parameters that apply to your router as a whole. Also, you can access the following modes, which are described later in this table: • Interface configuration • Router configuration • Line configuration

Table A-2 Command Modes Summary (continued)

Mode	Access Method	Prompt	Exit/Entrance Method	About this Mode
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. To exit to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**. 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.
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. 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. 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 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. 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. 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 #
```

Summary

Now that you have reviewed some Cisco IOS software basics, you can begin to configure your router. Remember:

- You can use the question mark (**?**) and arrow keys to help you enter commands.
- Each command mode restricts you to a set of commands. If you are having difficulty entering a command, check the prompt, and then enter the question mark (**?**) for a list of available commands. You might be in the wrong command mode or using the wrong syntax.

- 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, go to Chapter 3, "Basic Router Configuration," and Chapter 4, "Advanced Router Configuration."

APPENDIX B

ROM Monitor

This appendix describes the 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 documentation listed in the Obtaining Documentation section of this guide for information on connecting your 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	Purpose
Step 1	**enable**	If an enable password is configured, enters the enable command and the enable password to enter privileged EXEC mode.
Step 2	**configure terminal**	Enters global configuration mode.
Step 3	**config-reg 0x0**	Resets the configuration register.

	Command	Purpose
Step 4	**exit**	Exits global configuration mode.
Step 5	**reload**	Reboots the router with the new configuration register value. The router remains in ROM monitor and does not boot the Cisco IOS software. As long as the configuration value is 0x0, you must manually boot the operating system from the console. See the **boot** command in the "Command Descriptions" section in this appendix. After the router reboots, it is in ROM monitor mode. The number in the prompt increments with each new line.

Timesaver Break (system interrupt) is always enabled for 60 seconds after the router reboots, regardless of whether it is set to on or off in the configuration register. During this 60-second window, you can break to the ROM monitor prompt by pressing the Break key.

ROM Monitor Commands

Enter **?** or **help** at the ROM monitor prompt to display a list of available commands and options, as follows:

```
rommon 1 > ?
alias                   set and display aliases command
boot                    boot up an external process
break                   set/show/clear the breakpoint
confreg                 configuration register utility
cont                    continue executing a downloaded image
context                 display the context of a loaded image
cookie                  display contents of cookie PROM in hex
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:
	`rommon 16 > dis -?`
	`usage : dis [addr] [length]`
	The output for this command is slightly different for the **xmodem** download command:
	`rommon 11 > xmodem -?`
	`xmodem: illegal option -- ?`
	`usage: xmodem [-cyrxu] <destination filename>`
	`-c  CRC-16`
	`-y  ymodem-batch protocol`
	`-r  copy image to dram for launch`
	`-x  do not launch on download completion`
	`-u  upgrade ROMMON, System will reboot after upgrade`

reset or **i**	Resets and initializes the router, similar to a power up.

dev	Lists boot device identifications on the router; for example:
	`rommon 10> dev`
	`Devices in device table:`
	`        id  name`
	`    flash:  flash`

dir *device*:	Lists the files on the named device; for example, Flash files:
	`rommon 4 > dir flash:`
	`      File size           Checksum   File name`
	`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.

TFTP Download Command Variables

This section describes the system variables that can be set in ROM monitor mode and that are used during the TFTP download process. There are both required variables and optional variables.

Note The commands described in this section are case sensitive and must be entered exactly as shown.

Required Variables

These variables must be set with these commands before 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*

Variable	Command
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

These variables can be set with these commands before using the **tftpdnld** command:

Variable	Command
Configures how the router displays file download progress. **0**—No progress is displayed. **1**—Exclamation points (!!!) are displayed to indicate file download progress. This is the default setting. **2**—Detailed progress is displayed during the file download process; for example: • Initializing interface. • Interface link state up. • ARPing for 1.4.0.1 • ARP reply for 1.4.0.1 received. MAC address 00:00:0c:07:ac:01	**TFTP_VERBOSE=** *setting*
Number of times the router attempts ARP and TFTP download. The default is 7.	**TFTP_RETRY_COUNT=** *retry_times*
Amount of time, in seconds, before the download process times out. The default is 2,400 seconds (40 minutes).	**TFTP_TIMEOUT=** *time*
Whether or not the router performs a checksum test on the downloaded image: **1**—Checksum test is performed. **0**—No checksum test is performed.	**TFTP_CHECKSUM=***setting*

Using the TFTP Download Command

The steps described in this section should be performed while 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. 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 Trivial File Transfer Protocol (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: • Xmodem supports a 128-block transfer size. Ymodem supports a 1024-block transfer size. • Ymodem uses (CRC)-16 error checking to validate each packet. Depending on the device that the software is being downloaded from, this function might not be supported by Xmodem.
r	Optional. Image is loaded into DRAM for execution. 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 these steps 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 only displayed on the console 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 Cisco IOS software has crashed or is halted. If you enter a debugging command and Cisco IOS crash information is not available, you see the following error message:

```
"xxx: kernel context state is invalid, can not proceed."
```

The following are ROM monitor debugging commands:

- **stack** or **k**—produces a stack trace; for example:

```
rommon 6> stack
Stack trace:
PC = 0x801111b0
Frame 00: FP = 0x80005ea8    PC = 0x801111b0
Frame 01: FP = 0x80005eb4    PC = 0x80113694
Frame 02: FP = 0x80005f74    PC = 0x8010eb44
Frame 03: FP = 0x80005f9c    PC = 0x80008118
Frame 04: FP = 0x80005fac    PC = 0x80008064
Frame 05: FP = 0x80005fc4    PC = 0xfff03d70
```

- **context**—displays processor context; for example:

```
rommon 7> context
CPU context of the most recent exception:
PC  = 0x801111b0  MSR = 0x00009032  CR  = 0x53000035  LR    = 0x80113694
CTR = 0x801065e4  XER = 0xa0006d36  DAR = 0xffffffff  DSISR = 0xffffffff
DEC = 0xffffffff  TBU = 0xffffffff  TBL = 0xffffffff  IMMR  = 0xffffffff
R0  = 0x00000000  R1  = 0x80005ea8  R2  = 0xffffffff  R3    = 0x00000000
R4  = 0x8fab0d76  R5  = 0x80657d00  R6  = 0x80570000  R7    = 0x80570000
R8  = 0x00000000  R9  = 0x80570000  R10 = 0x0000954c  R11   = 0x00000000
R12 = 0x00000080  R13 = 0xffffffff  R14 = 0xffffffff  R15   = 0xffffffff
R16 = 0xffffffff  R17 = 0xffffffff  R18 = 0xffffffff  R19   = 0xffffffff
R20 = 0xffffffff  R21 = 0xffffffff  R22 = 0xffffffff  R23   = 0xffffffff
R24 = 0xffffffff  R25 = 0xffffffff  R26 = 0xffffffff  R27   = 0xffffffff
R28 = 0xffffffff  R29 = 0xffffffff  R30 = 0xffffffff  R31   = 0xffffffff
```

- **frame**—displays an individual stack frame.
- **sysret**—displays return information from the last booted system image. This information includes the reason for terminating the image, a stack dump of up to eight frames, and, if an exception is involved, the address where the exception occurred; for example:

```
rommon 8> sysret
System Return Info:
count: 19,  reason: user break
pc:0x801111b0,  error address: 0x801111b0
Stack Trace:
FP: 0x80005ea8, PC: 0x801111b0
FP: 0x80005eb4, PC: 0x80113694
FP: 0x80005f74, PC: 0x8010eb44
FP: 0x80005f9c, PC: 0x80008118
FP: 0x80005fac, PC: 0x80008064
FP: 0x80005fc4, PC: 0xfff03d70
FP: 0x80005ffc, PC: 0x00000000
FP: 0x00000000, PC: 0x00000000
```

- **meminfo**—displays size in bytes, starting address, available range of main memory, the starting point and size of packet memory, and size of NVRAM; for example:

```
rommon 9> meminfo
Main memory size: 40 MB.
Available main memory starts at 0x10000, size 40896KB
```

```
    IO (packet) memory size: 5 percent of main memory.
    NVRAM size: 32KB
```

Exiting the ROM Monitor

You must set the configuration register to a value from 0x2 to 0xF for the router to boot a Cisco IOS image from Flash memory upon startup or reloading.

The following example shows how to reset the configuration register and cause the router to boot a Cisco IOS image stored in Flash memory:

```
rommon 1 > confreg 0x2101


You must reset or power cycle for new config to take effect
rommon 2 >boot
```

The router will boot the Cisco IOS image in Flash memory. The configuration register will change to 0x2101 the next time the router is reset or power cycled.

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
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

Table C-1 Currently Assigned TCP and UDP Port Numbers (continued)

Port	Keyword	Description
77	–	Any private RJE service
79	FINGER	Finger
95	SUPDUP	SUPDUP Protocol
101	HOST NAME	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
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 UDP—rwho	TCP—UNIX rlogin UDP—UNIX broadcast name service
514	TCP—rsh UDP—syslog	TCP—UNIX rsh and log
515	Printer	UNIX line printer remote spooling
520	RIP	Routing Information Protocol
525	Timed	Time server

INDEX