Thank you for taking the time to fill out this response card. Your input is important to us and helps us to provide you with better documentation.

If you have comments about this document, please complete this self-addressed response card and mail it to us.

We also encourage you to make copies of this blank response card to complete and send to us whenever you have comments about this document. You can mail copies of this card to:

Cisco Systems, Inc.
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

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

You can also submit comments electronically on the World Wide Web. Click Feedback in the toolbar and select Documentation. After you complete the form, click Submit to send it to Cisco. We appreciate your comments.

---

Documentation Response Card


Please respond to the following statements by checking a number from 1 to 5:

5  Strongly agree
4  Somewhat agree
3  Neutral
2  Somewhat disagree
1  Strongly disagree

Overall, I am satisfied with this document.
Strongly agree 5  4  3  2  1  Strongly disagree

This document is accurate and free of errors.
Strongly agree 5  4  3  2  1  Strongly disagree

I can find the information I need in this document.
Strongly agree 5  4  3  2  1  Strongly disagree

This document is complete and offers enough relevant information for me to do my job.
Strongly agree 5  4  3  2  1  Strongly disagree

This document is written at the correct level of complexity for the subject matter.
Strongly agree 5  4  3  2  1  Strongly disagree

This document is useful to me in doing my job.
Strongly agree 5  4  3  2  1  Strongly disagree

Would you like us to contact you? Yes  No

Additional Information

Mailing Information

Date ________________________________
Company Name ________________________________
Contact Name ________________________________
Mailing Address ________________________________

City ________________________________ State/Province ________________________________
Zip/Postal Code ________________________________ Country ________________________________
Phone ( ) ________________________________ Extension ________________________________
Fax ( ) ________________________________ E-mail ________________________________
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 following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco’s installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco’s written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

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, EXPRESS 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, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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 following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco’s installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco’s written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

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, EXPRESS 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, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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 following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco’s installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco’s written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

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, EXPRESS 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.

Access Registrar, AccessPath, Any to Any, ATMDirector, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, CiscoConnect, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Technologies logo, ConnectWay, ControlStream, Fast Step, FireRunner, GigaStack, IIX, JumpStart, Kernel Proxy, MGX, Natural Network Viewer, NetSonar, Network Registrar, Packet, PIX, Point and Click Internetworking, Policy Builder, Precept, RouteStream, Secure Script, ServiceWay, SlideCast, SMARTnet, StreamView, The Cell, TrafficDirector, TransPath, ViewRunner, VirtualStream, VisionWay, VlanDirector, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and Asist, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Registrar, StrataView Plus, Stratem, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. (9905R)
About This Guide xi
Audience xi
Organization xi
Conventions xii
Terms xiii
Related Documentation xiv
References to Cisco IOS Documentation Set xv
Accessing Electronic Documentation xv

Chapter 1 Overview 1-1
Cisco 805 Router Overview 1-1
Sample Network Overview 1-2
How to Use Sample Networks 1-4
Deciding Which Sample Network to Use 1-4
WAN Options 1-5
WAN Encapsulation 1-6
Other Features 1-6
Routed and Routing Protocols 1-6
Easy IP (Phase 1) 1-7
Easy IP (Phase 2) 1-7
Firewall 1-8
NAT Overload 1-8
Configuration Options 1-9
Cisco 805 Fast Step Software 1-9
Cisco ConfigMaker Software 1-9
Cisco IOS Software 1-10
Network Management Support 1-10

Chapter 2 Cisco IOS Basic Skills 2-1
Configuring the Router from a PC 2-2
Understanding Command Modes 2-3
Getting Help 2-6
Enable Secret and Enable Passwords 2-7
Entering Global Configuration Mode 2-7
Using Commands 2-8
   Abbreviating Commands 2-8
   Undoing Commands 2-9
   Command-Line Error Messages 2-9
Saving Configuration Changes 2-10
Summary 2-10
Where to Go Next 2-10

Chapter 3 Configuring Remote Office to Corporate Office Networks 3-1
Before Configuring Networks 3-3
Network 1: Leased Line, HDLC 3-5
   Configuring the Cisco 805 Router 3-5
      Global Parameters 3-6
      Ethernet Interface 3-6
      Serial Interface 3-7
      Dynamic Routing 3-7
      Command-Line Access to the Router 3-8
   Configuring the Corporate Router 3-8
   Sample Configuration 3-8
Network 2: Leased Line, PPP 3-10
   Configuring the Cisco 805 Router 3-10
      Global Parameters 3-11
      Ethernet Interface 3-11
      Serial Interface 3-12
      Dynamic Routing 3-12
      Command-Line Access to the Router 3-13
   Configuring the Corporate Router 3-14
   Sample Configuration 3-14
Chapter 4 Configuring Small Office to ISP Networks 4-1

Before Configuring Networks 4-2

Network 1: Leased Line, PPP 4-3
Chapter 5  **Advanced Features**  5-1

- Configuring IP EIGRP  5-2
- Configuring Easy IP (Phase 1)  5-2
- Configuring Easy IP (Phase 2)  5-6
  - DHCP Server  5-7
  - DHCP Relay  5-8
- Configuring NAT Overload  5-10
Configuring the Firewall Feature 5-13
Configuring Windows NT 5-14
Controlling Dial-up Line Activation 5-15
  UDP Broadcasts in a Windows NT Environment 5-16
    Configuration 5-16
  UDP Broadcasts in a DHCP Relay Environment 5-17
    Configuration 5-18
  UDP Broadcasts in an SNTP Environment 5-18
    Configuration 5-19
IP Traffic 5-19
  Configuration 5-20
IPX Traffic 5-21
  Configuration 5-21
Restricting Access to Your IP Network 5-22
  Configuration 5-24

Chapter 6 Troubleshooting 6-1
  Verifying that Router Boots Properly 6-2
  Troubleshooting Physical Connections 6-3
    Ethernet Connection 6-3
    Serial Connection 6-4
  Troubleshooting Ethernet Line Problems 6-5
  Troubleshooting Serial Line Problems 6-6
    Synchronous CSU/DSU Clocking Problems 6-6
      Detecting Problems 6-6
      Performing Ping Tests 6-8
      Performing Loopback Tests 6-10
      Local Loopback Tests 6-11
      Remote Loopback Tests 6-12
    Synchronous Leased Line Problems 6-12
    Asynchronous Dial-up Problems 6-16
      Troubleshooting Problems with Modem and Router
      Connection 6-16
      No Connectivity between Modem and Router 6-18
Modem Does Not Dial 6-19
Modem Does Not Answer 6-21
Modem Hangs Up Shortly after Connecting 6-22
Dial-up Client Receives No EXEC Prompt 6-23
Dial-up Session Sees Garbage 6-25
Dial-up Session Ends Up in Existing Session 6-26
Modem Cannot Send or Receive Data 6-27
Modem Cannot Send or Receive IP Data 6-29
Modem Cannot Send or Receive IPX Data 6-31
Modem Does Not Disconnect Properly 6-32
Link Goes Deactivates Soon 6-33
Link Does Not Deactivate or Stays Activated Too Long 6-34
Poor Performance 6-35
Frame Relay Problems 6-36
Frame Relay Link is Down 6-36
Cannot Ping Remote Router 6-38
Cannot Ping End to End 6-40
X.25 Problems 6-41
No Connections over X.25 Link 6-41
Excess Serial Errors on X.25 Link 6-43
Using Debug Commands 6-44

Appendix A  ROM Monitor A-1
Using ROM Monitor A-1
ROM Monitor Modes A-2
Configuring Basic Configuration Parameters A-3
Commands A-6
Booting from a TFTP Server A-9

Appendix B  Upgrading the Software B-1
Upgrading Software from the CLI B-1
Upgrading Software from ROM Monitor B-3
Downloading Software from a TFTP Server B-5
Downloading Software from a Host Running XMODEM and a Terminal Emulator B-6
About This Guide

This section discusses the audience, organization, conventions, and terms and acronyms used in this guide. It also discusses related documentation and how to access electronic documentation.

Audience

This guide is intended for network administrators who have at least some experience configuring routers. This guide discusses how to configure the Cisco 805 router using the command-line interface (CLI) only. If you prefer not to use the CLI or are an inexperienced network administrator, Cisco recommends using the Cisco 805 Fast Step software to configure your router.

Organization

This guide contains the following information:

- About this Guide—Describes audience, organization, conventions, terms and acronyms, related documentation, and how to access electronic documentation.

- Overview—Provides overviews of the Cisco 805 router, sample networks in which the router is commonly used, and router configuration options.

- Cisco IOS Basic Skills—Describes what you need to know about the Cisco IOS software before you begin to configure it.

- Configuring Remote Office to Corporate Office Networks—Describes how to configure five commonly used remote-office-to-corporate-office networks.
• Configuring Small Office to ISP Networks—Describes how to configure three commonly used small-office-to-ISP networks.

• Advanced Features—Describes how to configure advanced features, such as Network Address Translation (NAT) overload, in your remote-office-to-corporate-office and small-office-to-ISP networks.

• Troubleshooting—Leads you through a troubleshooting checklist to determine the problem with your router. Also provides a solution to each problem.

• ROM Monitor—Describes the system software, its parameters and commands, and how to perform various tasks with it. Examples of tasks include deleting files from the Flash memory and configuring the router to boot from a Trivial File Transfer Protocol (TFTP) server.

• Upgrading the Software—Explains how to upgrade the version of Cisco IOS software running on your router.

• Concepts—Provides a comparison of available IP routing protocols and Point-to-Point Protocol (PPP) authentication protocols. Also provides information on the dialer profiles feature.

• Connecting Cisco Equipment to Other Vendor Equipment—Provides information on connecting your Cisco 805 router to routers manufactured by other vendors.

• Recovering a Lost Enable Password—Explains how to recover an enable password.

• Common Port Assignments—Describes the currently assigned Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) port numbers.

Conventions

This section describes the conventions used in this guide.

• The carat character (^) represents the Control key.

For example, the key combinations ^D and Ctrl-D are equivalent. Both mean hold down the Control key while you press the D key. Keys are indicated in capitals but are not case sensitive.
Command descriptions use these conventions:

- Commands and keywords are **boldface**.
- Variables for which you supply values are *italic*.
  - Elements in square brackets ([ ]) are optional.
  - Alternative but required keywords are grouped in braces ({ }) and separated by vertical bars (|).
- Examples use these conventions:
  - Terminal sessions and sample console screen displays are in `screen` font.
  - Information you enter is in **boldface screen** font.
  - Nonprinting characters, such as passwords, are in angle brackets (<>).
  - Default responses to system prompts are in square brackets ([ ]).

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

**Timesaver**  This symbol means the described action saves time. You can save time by performing the action described in the paragraph.

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

**Terms**

This section defines terms used in this guide.

**dial-up line**

A serial line that activates only when you need to access your WAN or when the router needs to send updates to other networking devices.
encapsulation
   The wrapping of data in a particular protocol header.

Interface
   A logical interface that you must configure to make the device attached to the port work.

partially meshed Frame Relay topology
   A topology where each router is not directly connected to every other router.

port
   A physical port on the router back panel.

private IP address
   An address that is not assigned by the Network Information Center (NIC) or an Internet service provider (ISP) and is therefore not globally unique.

public IP address
   A globally unique address assigned by the NIC or an ISP.

static routes
   A user-defined route to reach a particular destination.

Related Documentation

In addition to the Cisco 805 Router Software Configuration Guide, the Cisco 805 documentation set includes the following:

- Quick Start Guide—Setting Up the Cisco 805 Router
- Cisco 805 Router Hardware Installation Guide
References to Cisco IOS Documentation Set

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

- On the Documentation CD-ROM, select Cisco Product Documentation, select Cisco IOS Software Configuration, click Cisco IOS Release 12.0, and select one of the displayed links to find the desired document or feature.

- On CCO, go to Service and Support, and select Technical Document. Next, select Cisco Product Documentation, select Cisco IOS Software Configuration, click Cisco IOS Release 12.0, and select one of the displayed links to find the desired document or feature.

Accessing Electronic Documentation

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.
Overview

This chapter provides an overview of the Cisco 805 router, sample networks in which the router is commonly used, and router configuration options.

Cisco 805 Router Overview

The Cisco 805 router is designed for small professional offices and runs a subset of Cisco IOS software. This router includes one 10BaseT Ethernet port and one serial port, which can connect EIA/TIA-232, EIA/TIA-449, EIA/TIA-530, EIA/TIA-530A, X.21, and V.35 data terminal equipment (DTE) or data communications equipment (DCE).

You can connect a hub, server, PC, or workstation to the Ethernet port. The device that you connect to this port and the devices that are in turn connected to this device comprise your LAN.

A channel service unit/data service unit (CSU/DSU) and an asynchronous modem are the devices most commonly connected to the serial port. Both of these devices are DCE devices. The device that you connect to this port and the devices that are in turn connected to this device comprise your WAN.

Connect a CSU/DSU if you want to use a synchronous leased line, Frame Relay, or X.25, which are constantly active. Connect an asynchronous modem if you want your serial line to be a dial-up line. A dial-up line activates only when you need to access your WAN or when the router needs to send updates to other networking devices.
**Note**  Because a dial-up line is not constantly active, it is typically less expensive than a leased line, Frame Relay, or X.25. However, some protocols (IP, User Datagram Protocol [UDP], IPX, and Simple Network Time Protocol [SNTP]), send updates that can cause the dial-up line to be activated excessively. For information on preventing this situation, refer to “Controlling Dial-up Line Activation” in Chapter 5, “Advanced Features.”

For more details on connecting Ethernet and serial devices, refer to the *Cisco 805 Router Hardware Installation Guide*.

**Sample Network Overview**

Figure 1-1 and Figure 1-2 show sample networks in which the Cisco 805 router is commonly used.

**Figure 1-1 Remote Office to Corporate Office**

![Diagram of Remote Office to Corporate Office](image1.png)

**Figure 1-2 Small Office to ISP**

![Diagram of Small Office to ISP](image2.png)
In the remote-office-to-corporate-office sample network, the remote office is typically a small professional office that is part of a larger corporation, such as a real estate office. Although a majority of its data might exist at the remote office itself, the remote office might also need to exchange data with its larger corporate office. As a result, the remote office needs a connection to the corporate office.

In the small-office-to-Internet Service Provider (ISP) sample network, the small office is typically a small, independent professional office, such as an architectural firm. This type of office needs to access information from the Internet; therefore, it needs a connection to an ISP.

This guide presents several variations of these two sample networks. See Table 1-1 for a summary of the remote-office-to-corporate-office networks and Table 1-2 for a summary of the small-office-to-ISP networks presented in this guide.

The sample networks are ordered from simple to more complex in terms of concepts and configuration: remote-office-to-corporate-office network number 1 is the simplest, while network number 5 is the most complex.

### Table 1-1  Remote-Office-to-Corporate-Office Networks

<table>
<thead>
<tr>
<th>No.</th>
<th>WAN Options</th>
<th>WAN Encapsulation</th>
<th>Routed Protocols</th>
<th>Other Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Synchronous leased line</td>
<td>High-Level Data Link Control (HDLC)</td>
<td>IP</td>
<td>Dynamic IP routing</td>
</tr>
<tr>
<td>2</td>
<td>Synchronous leased line</td>
<td>Point-to-Point Protocol (PPP)</td>
<td>IP, IPX</td>
<td>Dynamic IP and IPX routing</td>
</tr>
<tr>
<td>3</td>
<td>X.25</td>
<td>X.25</td>
<td>IP, IPX</td>
<td>Dynamic IP and IPX routing</td>
</tr>
<tr>
<td>4</td>
<td>Asynchronous dial-up line</td>
<td>PPP</td>
<td>IP, IPX</td>
<td>Static IP and IPX routes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Easy IP (Phase 2) – DHCP server</td>
</tr>
<tr>
<td>5</td>
<td>Frame Relay</td>
<td>Frame Relay</td>
<td>IP, IPX</td>
<td>Partially meshed Frame Relay topology</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Subinterfaces</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Dynamic IP and IPX routing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Easy IP (Phase 2) – Dynamic Host Configuration Protocol (DHCP) relay</td>
</tr>
</tbody>
</table>
How to Use Sample Networks

The sample networks 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 sample networks or add or substitute features that better suit your needs.

Deciding Which Sample Network to Use

To determine which sample network best suits your needs, you must decide which WAN options (synchronous leased line, asynchronous dial-up line, Frame Relay, or X.25) to use. If you decide to use a synchronous leased line or an asynchronous dial-up line, you must also decide which WAN encapsulation protocol to use.

The following sections provide information to help you decide which WAN options and encapsulation to use.
Deciding Which Sample Network to Use

WAN Options

The most important factor in determining which sample network you use is the WAN option you choose (synchronous leased line, asynchronous dial-up line, Frame Relay, or X.25). Use the following criteria to help you decide which WAN option to use:

- Bandwidth requirements
- Cost
- Availability

To determine bandwidth requirements, you must consider the amount of data that will pass through your network and its speed. In general, an asynchronous modem (dial-up line) provides the least bandwidth, while a synchronous leased line provides the most bandwidth.

An asynchronous modem/dial-up line would probably suffice for a small professional office that needs to access the Internet a few times a day. However, a small office that needs to exchange large amounts of data with its corporate office throughout the day would probably need the higher throughput provided by a synchronous leased line or Frame Relay.

The monthly cost associated with your WAN options is an important factor. You can place the available WAN options into two categories:

- Lines that are constantly active, such as a synchronous leased line, a Frame Relay line, or an X.25 line
- Lines that are active on an as-needed basis, such as a dial-up line

In general, a dial-up line is the cheapest because it is not constantly active. Of the WAN options that offer constantly active lines, Frame Relay is the cheapest, then synchronous leased lines, then X.25 lines.

Note: Because a dial-up line is not constantly active, it is typically less expensive than a leased line, Frame Relay, or X.25. However, some protocols (IP, UDP, IPX, and SNTP), send updates that can cause the dial-up line to be activated excessively. For information on preventing this situation, refer to “Controlling Dial-up Line Activation” in Chapter 5, “Advanced Features.”
Sample Network Overview

Not all countries and regions have infrastructures for all WAN technologies. Therefore, your selection of WAN options might be limited by what is available. For example, X.25 might be the only WAN option supported in your country. If you are uncertain about your WAN options, contact the WAN service provider in your area.

WAN Encapsulation

If you decide to use a synchronous leased line or an asynchronous dial-up line, you must also decide what type of WAN encapsulation to use. Encapsulation is the wrapping of data in a particular protocol header. The type of router that you are connecting to the Cisco 805 router determines the type of WAN encapsulation. If the router you are connecting is a Cisco router that runs IOS software, use HDLC. If the router you are connecting is a Cisco router that does not run IOS software or is a non-Cisco router, use PPP.

Other Features

This section discusses the features used in the sample networks. You can choose not to use features presented in the sample networks or add or substitute features that better suit your needs.

Routed and Routing Protocols

In general, the remote-office-to-corporate-office sample networks use IP and IPX as the routed protocols. The exception is network 1 (synchronous leased line, HDLC), which is the simplest sample of this network type and uses IP only.

In general, the remote-office-to-corporate-office sample networks use the dynamic routing protocols IP RIP and IPX RIP to learn the route to the corporate office network. (Instead of using IP RIP, you can use IP EIGRP. IPX EIGRP is not supported.) The exception is network 4 (asynchronous dial-up line, PPP), which uses static IP and IPX routes, which are user-defined routes to reach the corporate office network.

The small-office-to-ISP networks use IP as the only routed protocol. Instead of using a dynamic routing protocol such as RIP to learn the route to the ISP, these networks use a static IP route to reach the ISP. In this situation, a dynamic routing protocol would advertise the small office network routes to the Internet, which is undesirable.
Easy IP (Phase 1)

Small-office-to-ISP network 2 (asynchronous dial-up line, PPP) uses the Easy IP (Phase 1) feature. Easy IP (Phase 1) combines NAT and PPP/Internet Protocol Control Protocol (PPP/IPCP).

For cost-effectiveness, this sample network assumes that the small office wants to buy as few registered IP addresses as possible from the Network Information Center (NIC) or the ISP. Instead, it will use private, nonregistered IP addresses everywhere except on the serial interface, which needs a registered IP address to access the ISP.

With PPP/IPCP, the Cisco 805 router automatically negotiates a globally unique (registered or public) IP address for the serial interface from the ISP router. With NAT, the Cisco 805 router translates the nonregistered IP addresses used by the small office network hosts into the globally unique IP address used by the serial interface when they access the Internet or vice versa.

For more information, see “Configuring Easy IP (Phase 1)” in Chapter 5, “Advanced Features.”

Easy IP (Phase 2)

Remote-office-to-corporate-office networks 4 and 5 (asynchronous dial-up line, PPP and Frame Relay, respectively) use the Easy IP (Phase 2) feature. Easy IP (Phase 2) combines Dynamic Host Configuration Protocol (DHCP) server and relay.

As an option, remote-office-to-corporate-office network 4 configures the Cisco 805 router as a DHCP server. The DHCP server assigns IP addresses to DHCP clients on the remote office network, thereby automating IP address administration.

Remote-office-to-corporate-office network 5 assumes that your corporate office network has a workstation or PC configured as a DHCP server and that DHCP clients on the remote office network need to access the DHCP server. If this situation applies to you, you can configure the DHCP relay feature on the Cisco 805 router. With this feature configured, the router can relay IP address requests from the LAN interface, over the serial or dialer interface, and to the DHCP server.

For more information, see “Configuring Easy IP (Phase 2)” in Chapter 5, “Advanced Features.”
Firewall

To configure a firewall, you must have one of the Cisco 805 software images that contain the firewall feature. For information on the firewall features that the Cisco 805 router supports, refer to the release notes that ship with the Cisco 805 router.

Small-office-to-ISP networks 2 and 3 (asynchronous dial-up line with PPP and Frame Relay, respectively) use the firewall feature to block undesired traffic from the ISP. To configure a firewall in these sample networks, you can use either the Cisco 805 Fast Step application (recommended for inexperienced network administrators) or the Cisco IOS software command-line interface (CLI) (recommended for more experienced network administrators).

If you want to configure a firewall in a remote-office-to-corporate-office network, you must use the Cisco IOS CLI.

For information on how to use the Cisco 805 Fast Step application, refer to the application online help. For information on how to configure a firewall using the CLI, refer to the Cisco IOS Firewall Feature Set feature module, which appears on Cisco Connection Online (CCO) only. This feature module also provides conceptual information on the firewall feature.

NAT Overload

Small-office-to-ISP network 3 (Frame Relay) uses the NAT overload feature. For cost-effectiveness, this sample network assumes that the small office wants to buy as few registered IP addresses as possible from the NIC or the ISP. Instead, it will use private, nonregistered IP addresses everywhere except on the serial interface, which needs a registered IP address to access the ISP.

You must buy one registered IP address for the serial interface from the ISP, then using NAT overload, all hosts in this sample network can use this registered IP address when accessing the Internet.

For more information, refer to the “Configuring NAT Overload” section in Chapter 5, “Advanced Features.”
Configuration Options

You can configure the router software using the following options:

- Cisco 805 Fast Step software
- Cisco ConfigMaker software
- Cisco IOS software

Cisco 805 Fast Step Software

Note Cisco recommends that inexperienced network administrators use the Cisco 805 Fast Step software to configure their routers.

The Cisco 805 Fast Step software is a Windows 95, Windows 98, and Windows NT based application that performs a basic configuration of your router. The Cisco 805 Fast Step software walks you through each step of the router configuration.

The Cisco 805 Fast Step software ships with the router; it is also available on Cisco Connection Online (CCO).

You can configure some of the sample networks described earlier in this chapter with Cisco 805 Fast Step. For more information, refer to Table 3-1 and Table 4-1.

Note The Cisco 805 Fast Step software might configure the sample networks differently than is described in this guide.

Cisco ConfigMaker Software

The Cisco ConfigMaker software is a Windows 95, Windows 98, and Windows NT based graphical application that can configure a small network of Cisco routers from a single PC, including the Cisco 805 router, switches, hubs, and other network devices. The Cisco
Network Management Support

ConfigMaker software is designed for resellers and network administrators of small- to medium-size businesses who are familiar with LAN fundamentals and basic network design.

You can access a free copy of the Cisco ConfigMaker software at this location:

http://www.cisco.com/pcgi-bin/tablebuild.pl/configmaker

Cisco IOS Software

The Cisco 805 router runs a subset of Cisco IOS software. Cisco recommends using the command-line interface (CLI) to configure your router if one of the following applies:

- You have previous experience configuring network devices.
- You have previous experience with Cisco IOS software.

You can configure all of the sample networks described earlier in this chapter by using the CLI.

If you need a refresher on how to use Cisco IOS software, go to Chapter 2, “Cisco IOS Basic Skills.” If you are ready to configure your router, go to Chapter 3, “Configuring Remote Office to Corporate Office Networks” or Chapter 4, “Configuring Small Office to ISP Networks.”

Network Management Support

The CiscoView software supports the Cisco 805 router. This software provides dynamic status, statistics, and comprehensive configuration information for Cisco switches, routers, concentrators, and adapters. It graphically displays a physical view of Cisco devices. This software also provides configuring and monitoring functions and offers basic troubleshooting.
Cisco IOS Basic Skills

Understanding how to use Cisco IOS software saves time when you are configuring your router. If you need a refresher, take a few minutes to read this chapter. If you are already familiar with Cisco IOS software, go to Chapter 3, “Configuring Remote Office to Corporate Office Networks” or Chapter 4, “Configuring Small Office to ISP Networks.”

This chapter describes what you need to know before you begin configuring your Cisco 805 router with Cisco IOS software (the software that runs your router).

*Note*  Cisco recommends that inexperienced network administrators use the Cisco 805 Fast Step software to configure their routers.

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
Configuring the Router from a PC

You can configure your router from a connected PC. For information on how to connect the PC, refer to the Cisco 805 Router Hardware Installation Guide.

After connecting the PC, you need terminal emulation software. The PC uses this software to send commands to your router. Table 2-1 lists some common types of this software, which are based on the type of PC you are using.

Table 2-1 Terminal Emulation Software

<table>
<thead>
<tr>
<th>PC Operating System</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 95, Windows 98, Windows NT</td>
<td>HyperTerm (included with Windows software), ProComm Plus</td>
</tr>
<tr>
<td>Windows 3.1</td>
<td>Terminal (included with Windows software)</td>
</tr>
<tr>
<td>Macintosh</td>
<td>ProComm, VersaTerm (supplied separately)</td>
</tr>
</tbody>
</table>

You can use the terminal emulation software to change settings for the type of device that is connected to the PC, in this case a router. Configure the software to the following standard VT-100 emulation settings so that your PC can communicate with your router:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit
- No flow control

These settings should match the default settings of your router. To change the router baud, data bits, parity, or stop bits settings, you must reconfigure parameters in the ROM monitor. For more information, refer to Appendix A, “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, refer to 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 2-2 lists the command modes that are used in this guide, how to access each mode, the prompt you see in that mode, and how to exit to a mode or enter the next mode. Because each mode configures different router elements, you might need to enter and exit modes frequently. You can see a list of available commands for a particular mode by entering a question mark (?) at the prompt. For a description of each command, including syntax, refer to the Cisco IOS 12.0 documentation set.
**Understanding Command Modes**

**Table 2-2 Command Modes Summary**

<table>
<thead>
<tr>
<th>Mode</th>
<th>Access Method</th>
<th>Prompt</th>
<th>Exit/Entrance Method</th>
<th>About this Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>User EXEC</td>
<td>Begin a session with your router.</td>
<td>Router&gt;</td>
<td>To exit router session, enter the logout command.</td>
<td>Use this mode to:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Change terminal settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Perform basic tests.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Display system information.</td>
</tr>
<tr>
<td>Privileged</td>
<td>Enter the enable command from user EXEC mode.</td>
<td>Router#</td>
<td>To exit to user EXEC mode, enter the disable command. To enter global configuration mode, enter the configure command.</td>
<td>Use this mode to:</td>
</tr>
<tr>
<td>EXEC</td>
<td></td>
<td></td>
<td></td>
<td>• Configure your router operating parameters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Perform the verification steps shown in this guide.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>
### Understanding Command Modes

#### Table 2-2 Command Modes Summary (continued)

<table>
<thead>
<tr>
<th>Mode</th>
<th>Access Method</th>
<th>Prompt</th>
<th>Exit/Entrance Method</th>
<th>About this Mode</th>
</tr>
</thead>
</table>
| 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. |                                               |
| 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. |                                                |
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-enable Create a temporary access-list entry
access-profile Apply user-profile to interface
clear Reset functions
...
```

To complete a command, enter a few known characters followed by a question mark (with no space):

```
router> 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
dialer Dialer parameters and statistics
exception exception information
...
```

Table 2-2 Command Modes Summary (continued)

<table>
<thead>
<tr>
<th>Mode</th>
<th>Access Method</th>
<th>Prompt</th>
<th>Exit/Entrance Method</th>
<th>About this Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Line configuration</td>
<td>Specify the line command with the desired keyword, for example, line 0, from global configuration mode.</td>
<td>Router (config-line)#</td>
<td>To exit to global configuration mode, enter the exit command.</td>
<td>Use this mode to configure parameters for the terminal line.</td>
</tr>
</tbody>
</table>

Getting Help
Enable Secret and Enable Passwords

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.

If you lose or forget your enable password, refer to Appendix E, “Recovering a Lost Enable Password.”

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 2-3 lists some error messages that you might encounter while using the CLI to configure your router.

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Meaning</th>
<th>How to Get Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>% Ambiguous command: &quot;show con&quot;</td>
<td>You did not enter enough characters for your router to recognize the command.</td>
<td>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.</td>
</tr>
<tr>
<td>% Incomplete command.</td>
<td>You did not enter all of the keywords or values required by this command.</td>
<td>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.</td>
</tr>
<tr>
<td>% Invalid input detected at `^' marker.</td>
<td>You entered the command incorrectly. The error occurred where the caret mark (^) appears.</td>
<td>Enter a question mark (?) to display all of the commands that are available in this command mode.</td>
</tr>
</tbody>
</table>
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 the Return key to accept the default destination filename startup-config, or enter your desired destination filename and press the Return key.

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 begin configuring your router, go to either Chapter 3, “Configuring Remote Office to Corporate Office Networks” or Chapter 4, “Configuring Small Office to ISP Networks.”
Configuring Remote Office to Corporate Office Networks

This chapter describes how to configure five remote-office-to-corporate-office networks, which Table 3-1 presents.

<table>
<thead>
<tr>
<th>No.</th>
<th>WAN Options</th>
<th>WAN Encapsulation</th>
<th>Routed Protocols</th>
<th>Other Features</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Synchronous leased</td>
<td>High-Level Data Link</td>
<td>IP</td>
<td>Dynamic IP routing</td>
<td>• Cisco 805 Fast Step software</td>
</tr>
<tr>
<td></td>
<td>leased line</td>
<td>Control (HDLC)</td>
<td></td>
<td></td>
<td>• Command-line interface (CLI)</td>
</tr>
<tr>
<td>2</td>
<td>Synchronous leased</td>
<td>Point-to-Point Protocol</td>
<td>IP, IPX</td>
<td>Dynamic IP and IPX routing</td>
<td>• Cisco 805 Fast Step software</td>
</tr>
<tr>
<td></td>
<td>leased line</td>
<td>(PPP)</td>
<td></td>
<td></td>
<td>• CLI</td>
</tr>
<tr>
<td>3</td>
<td>X.25</td>
<td>X.25</td>
<td>IP, IPX</td>
<td>Dynamic IP and IPX routing</td>
<td>CLI</td>
</tr>
<tr>
<td>4</td>
<td>Asynchronous</td>
<td>PPP</td>
<td>IP, IPX</td>
<td>Static IP and IPX routes</td>
<td>• Cisco 805 Fast Step software</td>
</tr>
<tr>
<td></td>
<td>dial-up line</td>
<td></td>
<td></td>
<td>Easy IP Phase 2 – DHCP server</td>
<td>(template option)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• CLI</td>
</tr>
</tbody>
</table>
Cisco strongly recommends that inexperienced network administrators use the Cisco 805 Fast Step software to configure sample networks 1, 2, and 5. The Cisco 805 Fast Step software might configure the sample networks differently than is described in this guide.

The Cisco 805 Fast Step software is a Windows 95, Windows NT, and Windows 98 based configuration tool included with the Cisco 805 router. For more information, refer to the Cisco 805 Fast Step CD-ROM.

For more information on configuring your router using the CLI, continue reading this chapter.

---

**Table 3-1 Sample Networks (continued)**

<table>
<thead>
<tr>
<th>No.</th>
<th>WAN Options</th>
<th>WAN Encapsulation</th>
<th>Routed Protocols</th>
<th>Other Features</th>
<th>Configuration Options</th>
</tr>
</thead>
</table>
| 5   | Frame Relay | Frame Relay       | IP, IPX          | • Partially meshed Frame Relay topology  
      |             |                   |                  | • Subinterfaces  
      |             |                   |                  | • Dynamic IP and IPX routing  
      |             |                   |                  | • Easy IP (Phase 2) – Dynamic Host Configuration Protocol (DHCP) relay | • Cisco 805 Fast Step software  
      |             |                   |                  |               | • CLI               |
Before Configuring Networks

Refer to Table 3-2 to determine what you need to do before configuring each network.

<table>
<thead>
<tr>
<th>Number</th>
<th>WAN Options/Encapsulation</th>
<th>What You Must Do(^1, 2)</th>
</tr>
</thead>
</table>
| 1      | Leased line, HDLC        | • Network administrators from corporate and remote offices:  
|        |                           |   — Set up IP address scheme.  
|        |                           |   — Decide which IP routing protocol to use.  
|        |                           | • Network administrator from corporate office must order leased line from WAN service provider. |
| 2      | Leased line, PPP          | • Network administrators from corporate and remote offices:  
|        |                           |   — Set up IP and IPX address scheme.  
|        |                           |   — Decide which IP routing protocol to use.  
|        |                           | • Network administrator from corporate office must order leased line from WAN service provider. |
| 3      | X.25                      | • Network administrators from corporate and remote offices:  
|        |                           |   — Set up IP and IPX address scheme.  
|        |                           |   — Decide which IP routing protocol to use.  
|        |                           | • Network administrator from corporate office must order X.25 connection from WAN service provider. Also, ask the WAN service provider to provide the following:  
|        |                           |   — X.25 address for remote office and corporate office router serial interfaces  
|        |                           |   — X.25 window size  
|        |                           |   — X.25 packet size |
Before Configuring Networks

Table 3-2  Before Configuring Networks (continued)

<table>
<thead>
<tr>
<th>Number</th>
<th>WAN Options/Encapsulation</th>
<th>What You Must Do¹, ²</th>
</tr>
</thead>
</table>
| 4      | Dial-up line, PPP         | • Network administrators from corporate and remote offices:  
|        |                           |   — Set up IP and IPX address scheme.  
|        |                           |   — Decide which IP routing protocol to use.  
|        |                           |   — Decide which PPP authentication type to use.  
|        |                           |   After deciding which PPP authentication type to use, you must decide on  
|        |                           |   a PPP client name and password to access the router.  
|        |                           |   — Provide telephone number assigned to the remote office router serial  
|        |                           |   interface to the corporate office network administrator and vice versa.  
|        |                           | • Network administrator from corporate office must order dial-up line from  
|        |                           |   WAN service provider.  
| 5      | Frame Relay               | • Network administrators from corporate and remote offices:  
|        |                           |   — Set up IP and IPX address scheme.  
|        |                           |   — Decide which IP routing protocol to use.  
|        |                           | • Network administrator from corporate office:  
|        |                           |   — Order two permanent virtual circuits (PVCs) from WAN service  
|        |                           |   provider. Provider should assign two data link connection identifiers  
|        |                           |   (DLCIs) for each PVC.  
|        |                           |   — Ask WAN service provider to provide Local Management Interface  
|        |                           |   (LMI) type.  

¹ For a comparison of IP Routing Information Protocol (RIP) and IP Enhanced Interior Gateway Routing Protocol (EIGRP), refer to the “Selecting IP Routing Protocols” section in Appendix C, “Concepts.”

² For a comparison of Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP), refer to the “Selecting PPP Authentication Protocol” section in Appendix C, “Concepts.”
Network 1: Leased Line, HDLC

Figure 3-1 shows a sample remote-office-to-corporate-office network with a synchronous leased line running HDLC. This sample network uses IP as the only routed protocol and RIP to learn the route to the corporate office network.

Configuring the Cisco 805 Router

To configure the features for this sample network, perform the tasks described in the following sections on a PC. A sample configuration file 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, refer to the “Entering Global Configuration Mode” section in Chapter 2, “Cisco IOS Basic Skills.” For more information on the commands used in the following tables, refer to the Cisco IOS Release 12.0 documentation set.
Global Parameters

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode.</td>
<td>Router#</td>
<td>configure terminal</td>
</tr>
<tr>
<td>2</td>
<td>Specify name for router.</td>
<td>Router (config)#</td>
<td>hostname name</td>
</tr>
<tr>
<td>3</td>
<td>Specify encrypted password to prevent unauthorized access to router.</td>
<td>Router (config)#</td>
<td>enable secret &lt;password&gt;</td>
</tr>
<tr>
<td>4</td>
<td>Configure router to recognize zero subnet range as valid range of addresses.</td>
<td>Router (config)#</td>
<td>ip subnet-zero</td>
</tr>
<tr>
<td>5</td>
<td>Disable router from translating unfamiliar words (typos) entered during a console session into IP addresses.</td>
<td>Router (config)#</td>
<td>no ip domain-lookup</td>
</tr>
</tbody>
</table>

Ethernet Interface

Use the following table to configure the Ethernet interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode for Ethernet interface.</td>
<td>Router (config)#</td>
<td>interface ethernet 0</td>
</tr>
<tr>
<td>2</td>
<td>Set IP address and subnet mask.</td>
<td>Router (config-if)#</td>
<td>ip address ip-address mask</td>
</tr>
<tr>
<td>3</td>
<td>Enable interface and configuration changes just made to interface.</td>
<td>Router (config-if)#</td>
<td>no shutdown</td>
</tr>
<tr>
<td>4</td>
<td>Exit configuration mode for Ethernet interface.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
</tbody>
</table>
Serial Interface

Use the following table to configure the serial interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode for serial interface.</td>
<td>Router (config)#</td>
<td>interface serial 0</td>
</tr>
<tr>
<td>2</td>
<td>Set IP address and subnet mask.</td>
<td>Router (config-if)#</td>
<td>ip address ip-address mask</td>
</tr>
<tr>
<td>3</td>
<td>Enable interface and configuration changes just made to interface.</td>
<td>Router (config-if)#</td>
<td>no shutdown</td>
</tr>
<tr>
<td>4</td>
<td>Exit configuration mode for serial interface.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
</tbody>
</table>

Dynamic Routing

This section describes how to configure RIP. For information on how to configure IP EIGRP, refer to the “Configuring IP EIGRP” section in Chapter 5, “Advanced Features.”

Use the following table to configure RIP.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter router configuration mode, and enable RIP.</td>
<td>Router (config)#</td>
<td>router rip</td>
</tr>
<tr>
<td>2</td>
<td>Specify use of RIP Version 2.</td>
<td>Router (config-router)#</td>
<td>version 2</td>
</tr>
<tr>
<td>3</td>
<td>Specify this command for each directly connected network.</td>
<td>Router (config-router)#</td>
<td>network network-number</td>
</tr>
<tr>
<td>4</td>
<td>Disable automatic summarization of subnet routes into network-level routes.</td>
<td>Router (config-router)#</td>
<td>no auto-summary</td>
</tr>
<tr>
<td>5</td>
<td>Exit router configuration mode.</td>
<td>Router (config-router)#</td>
<td>exit</td>
</tr>
</tbody>
</table>
Command-Line Access to the Router

Use the following table to configure parameters to control access to the router.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter line configuration mode, and specify the console terminal line.</td>
<td>Router (config)#</td>
<td>line console 0</td>
</tr>
<tr>
<td>2</td>
<td>Specify a unique password on the line.</td>
<td>Router (config-line)#</td>
<td>password &lt;password&gt;</td>
</tr>
<tr>
<td>3</td>
<td>Enable password checking at terminal session login.</td>
<td>Router (config-line)#</td>
<td>login</td>
</tr>
<tr>
<td>4</td>
<td>Set interval that EXEC command interpreter waits until user input is detected.</td>
<td>Router (config-line)#</td>
<td>exec-timeout 10 0</td>
</tr>
<tr>
<td>5</td>
<td>Specify a virtual terminal for remote console access.</td>
<td>Router (config-line)#</td>
<td>line vty 0 4</td>
</tr>
<tr>
<td>6</td>
<td>Specify a unique password on the line.</td>
<td>Router (config-line)#</td>
<td>password &lt;password&gt;</td>
</tr>
<tr>
<td>7</td>
<td>Enable password checking at virtual terminal session login.</td>
<td>Router (config-line)#</td>
<td>login</td>
</tr>
<tr>
<td>8</td>
<td>Exit line configuration mode, and return to privileged EXEC mode.</td>
<td>Router (config-line)#</td>
<td>end</td>
</tr>
</tbody>
</table>

Configuring the Corporate Router

This section assumes that the router connected to the Cisco 805 router is a Cisco router, such as a 3600 router. To configure the corporate router, use the same tasks as described in the “Configuring the Cisco 805 Router” section on page 3-5.

Sample Configuration

The following is a sample configuration based on performing the tasks in “Configuring the Cisco 805 Router” section on page 3-5. 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 command.
Sample Configuration

Current configuration:
!
version 12.0
no service pad (default)
service timestamps debug uptime (default)
service timestamps log uptime (default)
no service password-encryption (default)
hostname Cisco805
enable secret 5 $1$RnI.$K4mh5q4MFetaqKzBbQ7qv0
ip subnet-zero
no ip domain-lookup
!
interface Ethernet0
ip address 10.1.1.1 255.255.255.0
no ip directed-broadcast (default)
!
interface Serial0
ip address 30.1.1.1 255.255.255.0
no ip directed-broadcast (default)
no ip mroutecache (default)
!
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
Network 2: Leased Line, PPP

Figure 3-2 shows a sample remote-office-to-corporate-office network with a synchronous leased line running PPP. This sample network uses IP and IPX as the routed protocols and IP RIP and IPX RIP to learn the route to the corporate office network.

Figure 3-2 Network 2

Configuring the Cisco 805 Router

To configure the features for this sample network, perform the tasks described in the following sections on a PC. A sample configuration file 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, refer to the “Entering Global Configuration Mode” section in Chapter 2, “Cisco IOS Basic Skills.” For more information on the commands used in the following tables, refer to the Cisco IOS Release 12.0 documentation set.
Global Parameters

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode.</td>
<td>Router#</td>
<td>configure terminal</td>
</tr>
<tr>
<td>2</td>
<td>Specify name for router.</td>
<td>Router (config)#</td>
<td>hostname name</td>
</tr>
<tr>
<td>3</td>
<td>Specify encrypted password to prevent unauthorized access to router.</td>
<td>Router (config)#</td>
<td>enable secret &lt;password&gt;</td>
</tr>
<tr>
<td>4</td>
<td>Configure router to recognize zero subnet range as valid range of addresses.</td>
<td>Router (config)#</td>
<td>ip subnet-zero</td>
</tr>
<tr>
<td>5</td>
<td>Disable router from translating unfamiliar words (typos) entered during a console session into IP addresses.</td>
<td>Router (config)#</td>
<td>no ip domain-lookup</td>
</tr>
<tr>
<td>6</td>
<td>Enable IPX routing.</td>
<td>Router (config)#</td>
<td>ipx routing</td>
</tr>
</tbody>
</table>

Ethernet Interface

Use the following table to configure the Ethernet interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode for Ethernet interface.</td>
<td>Router (config)#</td>
<td>interface ethernet 0</td>
</tr>
<tr>
<td>2</td>
<td>Set IP address and subnet mask.</td>
<td>Router (config-if)#</td>
<td>ip address ip-address mask</td>
</tr>
<tr>
<td>3</td>
<td>Enable IPX routing, assign IPX network number, and configure encapsulation (framing) type.</td>
<td>Router (config-if)#</td>
<td>ipx network network encapsulation {arpa</td>
</tr>
<tr>
<td>4</td>
<td>Enable interface and configuration changes just made to interface.</td>
<td>Router (config-if)#</td>
<td>no shutdown</td>
</tr>
<tr>
<td>5</td>
<td>Exit configuration mode for Ethernet interface.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
</tbody>
</table>
Network 2: Leased Line, PPP

Serial Interface

Use the following table to configure the serial interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode for serial interface.</td>
<td>Router (config)#</td>
<td>interface serial 0</td>
</tr>
<tr>
<td>2</td>
<td>Set IP address and subnet mask.</td>
<td>Router (config-if)#</td>
<td>ip address ip-address mask</td>
</tr>
<tr>
<td>3</td>
<td>Enable IPX routing, and configure IPX network number.</td>
<td>Router (config-if)#</td>
<td>ipx network network</td>
</tr>
<tr>
<td>4</td>
<td>Specify PPP as encapsulation (framing) type.</td>
<td>Router (config-if)#</td>
<td>encapsulation ppp</td>
</tr>
<tr>
<td>5</td>
<td>Enable interface and configuration changes just made to interface.</td>
<td>Router (config-if)#</td>
<td>no shutdown</td>
</tr>
<tr>
<td>6</td>
<td>Exit configuration mode for serial interface.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
</tbody>
</table>

**Note** Although CHAP and PAP are not commonly used with a leased line, you can set them up on your serial interface to authenticate your connection to the corporate office router. For more information, refer to the “Selecting PPP Authentication Protocol” section in Appendix C, “Concepts.”

Dynamic Routing

This section describes how to configure IP RIP. (IPX RIP is enabled by default.) For information on how to configure IP EIGRP, refer to the “Configuring IP EIGRP” section in Chapter 5, “Advanced Features.”

Use the following table to configure IP RIP.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter router configuration mode, and enable RIP.</td>
<td>Router (config)#</td>
<td>router rip</td>
</tr>
<tr>
<td>2</td>
<td>Specify use of RIP Version 2.</td>
<td>Router (config-router)#</td>
<td>version 2</td>
</tr>
</tbody>
</table>

3-12 Cisco 805 Router Software Configuration Guide
### Configuring the Cisco 805 Router

#### Command-Line Access to the Router

Use the following table to configure parameters to control access to the router.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter line configuration mode, and specify the console terminal line.</td>
<td>Router (config)#</td>
<td>line console 0</td>
</tr>
<tr>
<td>2</td>
<td>Specify a unique password on the line.</td>
<td>Router (config-line)#</td>
<td>password &lt;password&gt;</td>
</tr>
<tr>
<td>3</td>
<td>Enable password checking at terminal session login.</td>
<td>Router (config-line)#</td>
<td>login</td>
</tr>
<tr>
<td>4</td>
<td>Set interval that EXEC command interpreter waits until user input is detected.</td>
<td>Router (config-line)#</td>
<td>exec-timeout 10 0</td>
</tr>
<tr>
<td>5</td>
<td>Specify a virtual terminal for remote console access.</td>
<td>Router (config-line)#</td>
<td>line vty 0 4</td>
</tr>
<tr>
<td>6</td>
<td>Specify a unique password on the line.</td>
<td>Router (config-line)#</td>
<td>password &lt;password&gt;</td>
</tr>
<tr>
<td>7</td>
<td>Enable password checking at virtual terminal session login.</td>
<td>Router (config-line)#</td>
<td>login</td>
</tr>
<tr>
<td>8</td>
<td>Exit line configuration mode, and return to privileged EXEC mode.</td>
<td>Router (config-line)#</td>
<td>end</td>
</tr>
</tbody>
</table>
Configuring the Corporate Router

This section assumes that the router connected to the Cisco 805 router is a Cisco router, such as a 3600 router. To configure the corporate router, use the same tasks as described in the “Configuring the Cisco 805 Router” section on page 3-10.

Sample Configuration

The following is a sample configuration based on performing the tasks in “Configuring the Cisco 805 Router” section on page 3-10. 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` command.

```
Current configuration:
!
version 12.0
no service pad (default)
service timestamps debug uptime (default)
service timestamps log uptime (default)
no service password-encryption (default)
hostname Cisco805
enable secret 5 $1$RnI.$K4mh5q4MFetaaqKzBbQ7qv0
ip subnet-zero
no ip domain-lookup
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 encapsulation novell-ether
!
interface Serial0
ip address 30.1.1.1 255.255.255.0
no ip directed-broadcast (default)
encapsulation ppp
no ip mroute-cache (default)
ipx network AAAA
!
router rip
version 2
network 10.0.0.0
```
Network 3: X.25

Figure 3-3 shows a sample remote office network connected to a corporate office network with X.25. This sample network uses IP and IPX as the routed protocols and IP RIP and IPX RIP to learn the route to the corporate office.

![Diagram of Network 3: X.25]

- **Network address:**
  - **IP:** 10.0.0.0
  - **IPX:** 100

- **Network address:**
  - **IP:** 30.0.0.0
  - **IPX:** AAAA

- **Network address:**
  - **IP:** 20.0.0.0
  - **IPX:** 200

Cisco 805 - Remote office

X.25

Cisco 3600 - Corporate office
Configuring the Cisco 805 Router

To configure the features for this sample network, perform the tasks described in the following sections on a PC. A sample configuration file 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, refer to the “Entering Global Configuration Mode” section in Chapter 2, “Cisco IOS Basic Skills.” For more information on the commands used in the following tables, refer to the Cisco IOS Release 12.0 documentation set.

Global Parameters

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode.</td>
<td>Router#</td>
<td>configure terminal</td>
</tr>
<tr>
<td>2</td>
<td>Specify name for router.</td>
<td>Router (config)#</td>
<td>hostname name</td>
</tr>
<tr>
<td>3</td>
<td>Specify encrypted password to prevent unauthorized access to router.</td>
<td>Router (config)#</td>
<td>enable secret &lt;password&gt;</td>
</tr>
<tr>
<td>4</td>
<td>Configure router to recognize zero subnet range as valid range of addresses.</td>
<td>Router (config)#</td>
<td>ip subnet-zero</td>
</tr>
<tr>
<td>5</td>
<td>Disable router from translating unfamiliar words (typos) entered during a console session into IP addresses.</td>
<td>Router (config)#</td>
<td>no ip domain-lookup</td>
</tr>
<tr>
<td>6</td>
<td>Enable IPX routing.</td>
<td>Router (config)#</td>
<td>ipx routing</td>
</tr>
</tbody>
</table>
Configuring the Cisco 805 Router

Ethernet Interface

Use the following table to configure the Ethernet interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode for Ethernet interface.</td>
<td>Router (config)#</td>
<td>interface ethernet 0</td>
</tr>
<tr>
<td>2</td>
<td>Set IP address and subnet mask.</td>
<td>Router (config-if)#</td>
<td>ip address ip-address mask</td>
</tr>
<tr>
<td>3</td>
<td>Enable IPX routing, assign IPX network number, and configure encapsulation (framing) type.</td>
<td>Router (config-if)#</td>
<td>ipx network network encapsulation {arpa</td>
</tr>
<tr>
<td>4</td>
<td>Enable interface and configuration changes just made to interface.</td>
<td>Router (config-if)#</td>
<td>no shutdown</td>
</tr>
<tr>
<td>5</td>
<td>Exit configuration mode for Ethernet interface.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
</tbody>
</table>

Serial Interface

Use the following table to configure the serial interface. This table provides basic X.25 commands to configure your serial interface to route IP and IPX packets over X.25. For information on other less commonly performed X.25-related tasks, refer to the Wide-Area Networking Configuration Guide.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode for serial interface.</td>
<td>Router (config)#</td>
<td>interface serial 0</td>
</tr>
<tr>
<td>2</td>
<td>Set IP address and subnet mask.</td>
<td>Router (config-if)#</td>
<td>ip address ip-address mask</td>
</tr>
<tr>
<td>3</td>
<td>Enable IPX routing, and configure IPX network number.</td>
<td>Router (config-if)#</td>
<td>ipx network network</td>
</tr>
<tr>
<td>4</td>
<td>Specify X.25 as encapsulation (framing) type.</td>
<td>Router (config-if)#</td>
<td>encapsulation x25</td>
</tr>
<tr>
<td>5</td>
<td>Set X.25 address (provided by your WAN service provider).</td>
<td>Router (config-if)#</td>
<td>x25 address address</td>
</tr>
</tbody>
</table>
Network 3: X.25

Dynamic Routing

This section describes how to configure IP RIP. (IPX RIP is enabled by default.) For information on how to configure IP EIGRP, refer to the “Configuring IP EIGRP” section in Chapter 5, “Advanced Features.”

Use the following table to configure IP RIP.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter router configuration mode, and enable RIP.</td>
<td>Router (config)#</td>
<td>router rip</td>
</tr>
<tr>
<td>2</td>
<td>Specify use of RIP Version 2.</td>
<td>Router (config-router)#</td>
<td>version 2</td>
</tr>
<tr>
<td>3</td>
<td>Specify this command for each directly connected network.</td>
<td>Router (config-router)#</td>
<td>network network-number</td>
</tr>
<tr>
<td>6</td>
<td>Enter this command once to set up LAN protocols-to-remote-host mapping for IP and X.25 and another time to set up mapping for IPX and X.25.</td>
<td>Router (config-if)#</td>
<td>x25 map protocol protocol-address x.121-address broadcast</td>
</tr>
<tr>
<td>7</td>
<td>Set network incoming window size (provided by your WAN service provider).</td>
<td>Router (config-if)#</td>
<td>x25 win packets</td>
</tr>
<tr>
<td>8</td>
<td>Set network outgoing window size (provided by your WAN service provider).</td>
<td>Router (config-if)#</td>
<td>x25 wout packets</td>
</tr>
<tr>
<td>9</td>
<td>Set network maximum input packet size (provided by your WAN service provider).</td>
<td>Router (config-if)#</td>
<td>x25 ips bytes</td>
</tr>
<tr>
<td>10</td>
<td>Set network maximum output packet size (provided by your WAN service provider).</td>
<td>Router (config-if)#</td>
<td>x25 ops bytes</td>
</tr>
<tr>
<td>11</td>
<td>Enable interface and configuration changes just made to interface.</td>
<td>Router (config-if)#</td>
<td>no shutdown</td>
</tr>
<tr>
<td>12</td>
<td>Exit configuration mode for serial interface.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
</tbody>
</table>
Configuring the Corporate Router

Command-Line Access to the Router

Use the following table to configure parameters to control access to the router.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter line configuration mode, and specify the console terminal line.</td>
<td>Router (config)#</td>
<td>line console 0</td>
</tr>
<tr>
<td>2</td>
<td>Specify a unique password on the line.</td>
<td>Router (config-line)#</td>
<td>password &lt;password&gt;</td>
</tr>
<tr>
<td>3</td>
<td>Enable password checking at terminal session login.</td>
<td>Router (config-line)#</td>
<td>login</td>
</tr>
<tr>
<td>4</td>
<td>Set interval that EXEC command interpreter waits until user input is detected.</td>
<td>Router (config-line)#</td>
<td>exec-timeout 10 0</td>
</tr>
<tr>
<td>5</td>
<td>Specify a virtual terminal for remote console access.</td>
<td>Router (config-line)#</td>
<td>line vty 0 4</td>
</tr>
<tr>
<td>6</td>
<td>Specify a unique password on the line.</td>
<td>Router (config-line)#</td>
<td>password &lt;password&gt;</td>
</tr>
<tr>
<td>7</td>
<td>Enable password checking at virtual terminal session login.</td>
<td>Router (config-line)#</td>
<td>login</td>
</tr>
<tr>
<td>8</td>
<td>Exit line configuration mode, and return to privileged EXEC mode.</td>
<td>Router (config-line)#</td>
<td>end</td>
</tr>
</tbody>
</table>

Configuring the Corporate Router

This section assumes that the router connected to the Cisco 805 router is a Cisco router, such as a 3600 router. To configure the corporate router, use the same tasks as described in the “Configuring the Cisco 805 Router” section on page 3-16.
Sample Configuration

The following is a sample configuration based on performing the tasks in “Configuring the Cisco 805 Router” section on page 3-16. 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 command.

While reviewing the following configuration, also refer to Figure 3-4, which illustrates the configuration specifics for mapping addresses between IP, IPX, and X.25.

```
Current configuration:
!
version 12.0
no service pad (default)
service timestamps debug uptime (default)
service timestamps log uptime (default)
no service password-encryption (default)
hostname Cisco805
enable secret 5 $1$RnI.$K4mh5q4MFetaqKzBbQ7gv0
ip subnet-zero
no ip domain-lookup
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)
no ip mroute-cache (default)
!
interface Serial0
ip address 30.1.1.1 255.255.255.0
no ip directed-broadcast (default)
encapsulation x25
no ip mroute-cache (default)
x25 address 31370054065
x25 win 7
x25 wout 7
x25 ips 512
x25 ops 512
x25 map ip 30.1.1.2 31370054066 broadcast
x25 map ipx AAAA.0010.7b7e.5598 31370054066 broadcast
```
In the two preceding commands, you map the IP and IPX addresses assigned to the corporate office router serial interface to the X.25 address assigned to the corporate office router serial interface. See Figure 3-4.

```
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
```

Figure 3-4 Sample X.25 Network

<table>
<thead>
<tr>
<th>IP address: 30.1.1.1</th>
<th>IP address: 30.1.1.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPX address: AAAA.0010.7b7e.5599</td>
<td>IPX address: AAAA.0010.7b7e.5598</td>
</tr>
<tr>
<td>X.25 address: 31370054065</td>
<td>X.25 address: 31370054066</td>
</tr>
</tbody>
</table>

Cisco 805  X.25  Cisco 3600

Remote office  Corporate office
Network 4: Dial-up Line, PPP

Figure 3-5 shows a sample remote office network connected to a corporate office network with an asynchronous dial-up line running PPP. This sample network uses IP and IPX as the routed protocols. Instead of using dynamic routing protocols such as IP and IPX RIP to learn the route to the corporate network, this network uses static IP and IPX routes, which are user-defined routes to the corporate network.

This sample network uses the dial-on-demand routing (DDR) implementation of dialer profiles. For more information, refer to the “Dialer Profiles” section in Appendix C, “Concepts.”

You can also configure the Cisco 805 router as a DHCP server. (The DHCP server feature is part of Easy IP [Phase 2]). A DHCP server allocates IP addresses from a central pool to DHCP clients on the remote office network.

Configuring the Cisco 805 Router

To configure the features for this sample network, perform the tasks described in the following sections on a PC. A sample configuration file 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, refer to the “Entering Global Configuration Mode” section in Chapter 2, “Cisco IOS Basic Skills.” For more information on the commands used in the following tables, refer to the Cisco IOS Release 12.0 documentation set.

Global Parameters

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode.</td>
<td>Router#</td>
<td>configure terminal</td>
</tr>
<tr>
<td>2</td>
<td>Specify name for router.</td>
<td>Router (config)#</td>
<td>hostname name</td>
</tr>
<tr>
<td>3</td>
<td>Specify encrypted password to prevent unauthorized access to router.</td>
<td>Router (config)#</td>
<td>enable secret &lt;password&gt;</td>
</tr>
<tr>
<td>4</td>
<td>Specify username and password used during caller identification and PAP and CHAP authentication. Username and password entered with this command must match hostname and password on corporate router.</td>
<td>Router (config)#</td>
<td>username name password &lt;secret&gt;</td>
</tr>
<tr>
<td>5</td>
<td>Configure router to recognize zero subnet range as valid range of addresses.</td>
<td>Router (config)#</td>
<td>ip subnet-zero</td>
</tr>
<tr>
<td>6</td>
<td>Disable router from translating unfamiliar words (typos) entered during a console session into IP addresses.</td>
<td>Router (config)#</td>
<td>no ip domain-lookup</td>
</tr>
<tr>
<td>7</td>
<td>Enable IPX routing.</td>
<td>Router (config)#</td>
<td>ipx routing</td>
</tr>
<tr>
<td>8</td>
<td>Specify static SAP entries. For more information on SAP types, refer to your Novell NetWare documentation.</td>
<td>Router (config)#</td>
<td>ipx sap service-type name network.node socket hop-count</td>
</tr>
</tbody>
</table>
### Ethernet Interface

Use the following table to configure the Ethernet interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode for Ethernet interface.</td>
<td>Router (config)#</td>
<td>interface ethernet 0</td>
</tr>
<tr>
<td>2</td>
<td>Set IP address and subnet mask.</td>
<td>Router (config-if)#</td>
<td>ip address ip-address mask</td>
</tr>
<tr>
<td>3</td>
<td>Enable IPX routing, assign IPX network number, and configure encapsulation (framing) type.</td>
<td>Router (config-if)#</td>
<td>ipx network network encapsulation {arpa</td>
</tr>
<tr>
<td>4</td>
<td>Enable interface and configuration changes just made to interface.</td>
<td>Router (config-if)#</td>
<td>no shutdown</td>
</tr>
<tr>
<td>5</td>
<td>Exit configuration mode for Ethernet interface.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
</tbody>
</table>

### Serial Interface

Use the following table to configure the serial interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode for serial interface.</td>
<td>Router (config)#</td>
<td>interface serial 0</td>
</tr>
<tr>
<td>2</td>
<td>Disable IP processing.</td>
<td>Router (config-if)#</td>
<td>no ip address</td>
</tr>
<tr>
<td>3</td>
<td>Specify PPP as encapsulation (framing) type.</td>
<td>Router (config-if)#</td>
<td>encapsulation ppp</td>
</tr>
<tr>
<td>4</td>
<td>Enable CHAP and/or PAP.</td>
<td>Router (config-if)#</td>
<td>ppp authentication chap pap or</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ppp authentication chap</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ppp authentication pap</td>
</tr>
<tr>
<td>5</td>
<td>Specify mode of serial interface as asynchronous.</td>
<td>Router (config-if)#</td>
<td>physical-layer async</td>
</tr>
<tr>
<td>6</td>
<td>Configure asynchronous line for data traffic.</td>
<td>Router (config-if)#</td>
<td>async mode dedicated</td>
</tr>
</tbody>
</table>
Configuring the Cisco 805 Router

Dialer Profile

To configure the dialer profile, you must set up a dialer interface and dialer pool. (The dialer pool is set up with the serial interface.) For conceptual information, refer to the “Dialer Profiles” section in Appendix C, “Concepts.”

Use the following table to configure the dialer interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode for and define dialer rotary group.</td>
<td>Router (config)#</td>
<td>interface dialer 1</td>
</tr>
<tr>
<td>2</td>
<td>Set IP address and subnet mask.</td>
<td>Router (config)#</td>
<td>ip address ip-address mask</td>
</tr>
<tr>
<td>3</td>
<td>Specify PPP as encapsulation (framing) type.</td>
<td>Router (config)#</td>
<td>encapsulation ppp</td>
</tr>
<tr>
<td>4</td>
<td>Enable CHAP and/or PAP.</td>
<td>Router (config)#</td>
<td>ppp authentication chap pap or ppp authentication chap or ppp authentication pap</td>
</tr>
<tr>
<td>5</td>
<td>Specify corporate office router authentication name.</td>
<td>Router (config)#</td>
<td>dialer remote-name name</td>
</tr>
<tr>
<td>6</td>
<td>Specify amount of idle time before calls are disconnected.</td>
<td>Router (config)#</td>
<td>dialer idle-timeout seconds</td>
</tr>
</tbody>
</table>
### Network 4: Dial-up Line, PPP

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Specify telephone number of corporate office router.</td>
<td>Router (config-if)#</td>
<td>dialer string string</td>
</tr>
<tr>
<td>8</td>
<td>Specify dialer pool to use for calls to corporate office. (Dialer pool was set up in “Serial Interface” section on page 3-24.)</td>
<td>Router (config-if)#</td>
<td>dialer pool number</td>
</tr>
<tr>
<td>9</td>
<td>Assign dialer interface to a dialer group.</td>
<td>Router (config-if)#</td>
<td>dialer-group number</td>
</tr>
<tr>
<td>10</td>
<td>Disable CDP.</td>
<td>Router (config-if)#</td>
<td>no cdp enable</td>
</tr>
<tr>
<td>11</td>
<td>Enable IPX routing, and configure IPX network number.</td>
<td>Router (config-if)#</td>
<td>ipx network network</td>
</tr>
<tr>
<td>12</td>
<td>Disable IPX fast switching.</td>
<td>Router (config-if)#</td>
<td>no ipx route-cache</td>
</tr>
<tr>
<td>13</td>
<td>Configure router to respond to watchdog packets of a server on behalf of a remote client.</td>
<td>Router (config-if)#</td>
<td>ipx watchdog-spoof</td>
</tr>
<tr>
<td>14</td>
<td>Configure router to respond to client or server SPX keepalive packets on behalf of a remote system.</td>
<td>Router (config-if)#</td>
<td>ipx spx-spoof</td>
</tr>
<tr>
<td>15</td>
<td>Exit configuration mode for dialer interface.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
<tr>
<td>16</td>
<td>Set up IP static route to corporate router.</td>
<td>Router (config)#</td>
<td>ip route destination-network destination-subnet-mask next-hop</td>
</tr>
<tr>
<td>17</td>
<td>Create script that causes connected modem to place call to other corporate route.</td>
<td>Router (config)#</td>
<td>chat-script script-name expect-send</td>
</tr>
<tr>
<td>18</td>
<td>Set up IPX static route to corporate router.</td>
<td>Router (config)#</td>
<td>ipx route network next-hop</td>
</tr>
<tr>
<td>19</td>
<td>Set up dialer list that determines which protocols trigger a call. (Enter one command for each protocol that you want to permit.)</td>
<td>Router (config)#</td>
<td>dialer-list dialer-group protocol protocol-name permit</td>
</tr>
</tbody>
</table>

For information on controlling the types of traffic that can activate your dial-up line and increase your monthly dial-up line cost, refer to the “Controlling Dial-up Line Activation” section in Chapter 5, “Advanced Features.”
Configuring the Cisco 805 Router

Asynchronous Line

Use the following table to configure the asynchronous line.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode for asynchronous line (line 1).</td>
<td>Router (config)#</td>
<td>line 1</td>
</tr>
<tr>
<td>2</td>
<td>Set hardware flow control.</td>
<td>Router (config-line)#</td>
<td>flowcontrol hardware</td>
</tr>
<tr>
<td>3</td>
<td>Specify that all protocols can connect to line 1.</td>
<td>Router (config-line)#</td>
<td>transport input all</td>
</tr>
<tr>
<td>4</td>
<td>Configure line 1 for both incoming and outgoing calls.</td>
<td>Router (config-line)#</td>
<td>modem inout</td>
</tr>
<tr>
<td>5</td>
<td>Set baud rate.</td>
<td>Router (config-line)#</td>
<td>speed 115200</td>
</tr>
<tr>
<td>6</td>
<td>Set stop bits.</td>
<td>Router (config-line)#</td>
<td>stopbits 1</td>
</tr>
<tr>
<td>7</td>
<td>Exit asynchronous line configuration mode.</td>
<td>Router (config-line)#</td>
<td>exit</td>
</tr>
</tbody>
</table>

DHCP Server

For information on configuring the Cisco 805 router as a DHCP server, refer to the “DHCP Server” section in Chapter 5, “Advanced Features.”

Command-Line Access to the Router

Use the following table to configure parameters to control access to the router.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter line configuration mode, and specify the console terminal line.</td>
<td>Router (config)#</td>
<td>line console 0</td>
</tr>
<tr>
<td>2</td>
<td>Specify a unique password on the line.</td>
<td>Router (config-line)#</td>
<td>password &lt;password&gt;</td>
</tr>
<tr>
<td>3</td>
<td>Enable password checking at terminal session login.</td>
<td>Router (config-line)#</td>
<td>login</td>
</tr>
<tr>
<td>4</td>
<td>Set interval that EXEC command interpreter waits until user input is detected.</td>
<td>Router (config-line)#</td>
<td>exec-timeout 10 0</td>
</tr>
</tbody>
</table>
Configuring the Corporate Router

This section assumes that the router connected to the Cisco 805 router is a Cisco router, such as a Cisco 3600 router. To configure the corporate router, use the same tasks as described in the “Configuring the Cisco 805 Router” section on page 3-22 except do not configure the corporate router as a DHCP server.

Sample Configuration

The following is a sample configuration based on performing the tasks in “Configuring the Cisco 805 Router” section on page 3-22. 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` command.
Sample Configuration

Current configuration:
!
version 12.0
no service pad (default)
service timestamps debug uptime (default)
service timestamps log uptime (default)
no service password-encryption (default)
hostname Cisco805
enable secret 5 $1$RnI.$K4mh5q4MFetgKzbBbQ7gv0
username Cisco3600 password abracadabra
ip subnet-zero
!
ip dhcp pool dhcppool_1
network 10.1.1.1 255.255.255.0
default-router 10.1.1.1
!
no ip domain-lookup
ipx routing 0010.7b7e.5499
!In the preceding command, the router MAC address is automatically used
!as the router IPX address.
chat-script dial "" AT OK "\patdt\T" TIMEOUT 60 CONNECT \C
!This generic chat script is known to work. For information on
!customizing your chat script, refer to the Dial Solutions Configuration
!Guide.

interface Ethernet0
ip address 10.1.1.1 255.255.255.0
no ip directed-broadcast (default)
ipx network 100 encapsulation novell-ether
!
interface Serial0
physical-layer async
no ip address
no ip directed-broadcast (default)
encapsulation ppp
dialer in-band
dialer pool-member 1
async default routing
async mode dedicated
ppp authentication chap pap
!
interface Dialer1
ip address 30.1.1.1 255.255.255.0
no ip directed-broadcast (default)
encapsulation ppp
dialer remote-name Cisco3600
dialer idle-timeout 500
dialer string 5551111
dialer pool 1
dialer-group 1
ipx network AAAA
no ipx route-cache
ipx watchdog-spoof
ipx spx-spoof
no cdp enable
ppp authentication chap pap
!
no ip http server (default)
ip classless (default)
!
ip route 20.1.1.0 255.255.255.0 30.1.1.2
ipx route 200 AAAA.0010.7b7e.5477
ipx sap 4 corporate-server 200.0020.0c00.75ec 452 1
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
line con 0
eexec-timeout 10 0
password 4youreyesonly
login
transport input none (default)
stopbits 1 (default)
line 1
modem InOut
transport input all
speed 115200
flowcontrol hardware
line vty 0 4
password secret
login
!
end
Network 5: Frame Relay

Figure 3-6 shows a sample remote-office-to-corporate-office network that uses Frame Relay. This sample network uses IP and IPX as the routed protocols and IP and IPX RIP to learn the routes to the corporate network.

This sample network uses a partially meshed Frame Relay topology, which means that each router is not directly connected to every other router. In this network, the remote office routers are not directly connected. However, serial interface 0 on the corporate office router is divided into virtual subinterfaces so that the remote office routers can communicate.
through the corporate office router. Each subinterface has a *permanent virtual circuit* (PVC) associated with it. For more information on partially meshed topologies, subinterfaces, and PVCs, refer to the Cisco IOS Release 12.0 documentation set.

The corporate network also has a PC or workstation that runs DHCP (*a DHCP server*). The DHCP server provides IP addresses to LAN devices on the remote networks (*DHCP clients*). You can set up the DHCP relay feature on the Cisco 805 router so that it relays DHCP client requests for IP addresses from the LAN interface, over the serial interface, and to the DHCP server. The DHCP relay feature is part of Easy IP (Phase 2).

### Configuring the Cisco 805 Routers

To configure the features for this sample network, perform the tasks described in the following sections on a PC. A sample configuration file 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, refer to the “Entering Global Configuration Mode” section in Chapter 2, “Cisco IOS Basic Skills.” For more information on the commands used in the following tables, refer to the Cisco IOS Release 12.0 documentation set.

### Global Parameters

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode.</td>
<td>Router#</td>
<td>configure terminal</td>
</tr>
<tr>
<td>2</td>
<td>Specify name for router.</td>
<td>Router (config)#</td>
<td>hostname name</td>
</tr>
<tr>
<td>3</td>
<td>Specify encrypted password to prevent</td>
<td>Router (config)#</td>
<td>enable secret &lt;password&gt;</td>
</tr>
<tr>
<td></td>
<td>unauthorized access to router.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Configure router to recognize zero subnet</td>
<td>Router (config)#</td>
<td>ip subnet-zero</td>
</tr>
<tr>
<td></td>
<td>range as valid range of addresses.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring the Cisco 805 Routers

#### Ethernet Interface

Use the following table to configure the Ethernet interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode for Ethernet interface.</td>
<td>Router (config)#</td>
<td>interface ethernet 0</td>
</tr>
<tr>
<td>2</td>
<td>Set IP address and subnet mask.</td>
<td>Router (config-if)#</td>
<td>ip address ip-address mask</td>
</tr>
<tr>
<td>3</td>
<td>Enable IPX routing, assign IPX network number, and configure encapsulation (framing) type.</td>
<td>Router (config-if)#</td>
<td>ipx network network encapsulation {arp</td>
</tr>
<tr>
<td>4</td>
<td>Enable interface and configuration changes just made to interface.</td>
<td>Router (config-if)#</td>
<td>no shutdown</td>
</tr>
<tr>
<td>5</td>
<td>Exit configuration mode for Ethernet interface.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
</tbody>
</table>

#### Serial Interface

Use the following table to configure the serial interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode for serial interface.</td>
<td>Router (config)#</td>
<td>interface serial 0</td>
</tr>
<tr>
<td>2</td>
<td>Set IP address and subnet mask.</td>
<td>Router (config-if)#</td>
<td>ip address ip-address mask</td>
</tr>
<tr>
<td>3</td>
<td>Enable IPX network, and configure IPX network number.</td>
<td>Router (config-if)#</td>
<td>ipx network network</td>
</tr>
</tbody>
</table>

---

**Configuring Remote Office to Corporate Office Networks**  
3-33
Dynamic Routing

This section describes how to configure IP RIP. (IPX RIP is enabled by default.) For information on how to configure IP EIGRP, refer to the “Configuring IP EIGRP” section in Chapter 5, “Advanced Features.”

Use the following table to configure IP RIP.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter router configuration mode, and enable RIP.</td>
<td>Router (config)#</td>
<td>router rip</td>
</tr>
<tr>
<td>2</td>
<td>Specify use of RIP Version 2.</td>
<td>Router (config-router)#</td>
<td>version 2</td>
</tr>
<tr>
<td>3</td>
<td>Specify this command for each directly connected network.</td>
<td>Router (config-router)#</td>
<td>network network-number</td>
</tr>
<tr>
<td>4</td>
<td>Disable automatic summarization of subnet routes into network-level routes.</td>
<td>Router (config-router)#</td>
<td>no auto-summary</td>
</tr>
<tr>
<td>5</td>
<td>Exit router configuration mode.</td>
<td>Router (config-router)#</td>
<td>exit</td>
</tr>
</tbody>
</table>

DHCP Relay

For information on configuring DHCP relay, refer to the “DHCP Relay” section in Chapter 5, “Advanced Features.”

3-34  Cisco 805 Router Software Configuration Guide
Command-Line Access to the Routers

Use the following table to configure parameters to control access to the router.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter line configuration mode, and specify the console terminal line.</td>
<td>Router (config)#</td>
<td>line console 0</td>
</tr>
<tr>
<td>2</td>
<td>Specify a unique password on the line.</td>
<td>Router (config-line)#</td>
<td>password &lt;password&gt;</td>
</tr>
<tr>
<td>3</td>
<td>Enable password checking at terminal session login.</td>
<td>Router (config-line)#</td>
<td>login</td>
</tr>
<tr>
<td>4</td>
<td>Set interval that EXEC command interpreter waits until user input is detected.</td>
<td>Router (config-line)#</td>
<td>exec-timeout 10 0</td>
</tr>
<tr>
<td>5</td>
<td>Specify a virtual terminal for remote console access.</td>
<td>Router (config-line)#</td>
<td>line vty 0 4</td>
</tr>
<tr>
<td>6</td>
<td>Specify a unique password on the line.</td>
<td>Router (config-line)#</td>
<td>password &lt;password&gt;</td>
</tr>
<tr>
<td>7</td>
<td>Enable password checking at virtual terminal session login.</td>
<td>Router (config-line)#</td>
<td>login</td>
</tr>
<tr>
<td>8</td>
<td>Exit line configuration mode, and return to privileged EXEC mode.</td>
<td>Router (config-line)#</td>
<td>end</td>
</tr>
</tbody>
</table>

Configuring the Corporate Router

This section assumes that the corporate router is a Cisco router, such as a 3600 router. To configure the corporate router, use the same tasks as described in the “Configuring the Cisco 805 Routers” section on page 3-32. There are some differences in how you configure the corporate router:

- Instead of setting an IP address and subnet address for the serial interface, specify the **no ip address** command in serial interface configuration mode. Do not specify an IPX address. (Instead, you set IP and IPX addresses for the serial subinterfaces.)
- Configure two serial subinterfaces after you finish configuring the serial interface.
- Do not configure the DHCP relay feature.
Use the following table to configure each subinterface. (The sample network uses two subinterfaces (0.1 and 0.2); therefore, you must perform the steps in the following table twice.)

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode for the serial subinterface, and specify interface as a point-to-point connection.</td>
<td>Router (config)#</td>
<td>interface serial interface.subinterface point-to-point</td>
</tr>
<tr>
<td>2</td>
<td>Set IP address and subnet mask.</td>
<td>Router (config-if)#</td>
<td>ip address ip-address mask</td>
</tr>
<tr>
<td>3</td>
<td>Enable IPX network, and configure IPX network number.</td>
<td>Router (config-if)#</td>
<td>ipx network network</td>
</tr>
<tr>
<td>4</td>
<td>Associate a DLCI with subinterface.</td>
<td>Router (config-if)#</td>
<td>frame-relay interface-dlci dlci</td>
</tr>
<tr>
<td>5</td>
<td>Exit configuration mode for serial interface.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
</tbody>
</table>

Sample Cisco 805 Routers Configurations

The following are sample configurations for the Cisco 805 A and Cisco 805 B routers, respectively, which are shown in Figure 3-6. These configurations are based on performing the tasks in “Configuring the Cisco 805 Routers” section on page 3-32. 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` command.

Current configuration:

```
Current configuration:
!
version 12.0
no service pad (default)
service timestamps debug uptime (default)
service timestamps log uptime (default)
no service password-encryption (default)
hostname Cisco805A
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 Serial0
ip address 30.1.1.1 255.255.255.0
ip helper-address 20.1.1.2
no ip directed-broadcast (default)
encapsulation frame-relay
no ip mroute-cache (default)
ipx network AAAA
frame-relay lmi-type ansi
!
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
Current configuration:
!
version 12.0
no service pad (default)
service timestamps debug uptime (default)
service timestamps log uptime (default)
no service password-encryption (default)
hostname Cisco805B
enable secret 6 %tu0jue\we940./7
ip subnet-zero
no ip domain-lookup
ip dhcp-server 20.1.1.2
ipx routing 0010.7b7e.5497
! In the preceding command, the router MAC address is automatically used as the router IPX address.
!
interface Ethernet0
ip address 40.1.1.1 255.255.255.0
no ip directed-broadcast (default)
ipx network 400
!
interface Serial0
ip address 30.2.1.1 255.255.255.0
ip helper-address 20.1.1.2
no ip directed-broadcast (default)
encapsulation frame-relay
no ip mroute-cache (default)
ipx network BBBB
frame-relay lmi-type ansi
!
router rip
version 2
network 30.0.0.0
network 40.0.0.0
no auto-summary
!
no ip http server (default)
ip classless (default)
!
line con 0
eexec-timeout 10 0
password 4youreyesonly
login
transport input none (default)
stopbits 1 (default)
Sample Cisco 3600 Router Configuration

The following is a sample configuration for the Cisco 3600 router. This configuration is based on performing the tasks in “Configuring the Corporate Router” section on page 3-35. 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` command.

While reviewing the following configuration, also refer to Figure 3-7, which shows the configuration specifics for the Cisco 3600 router.

```plaintext
Current configuration:
!
version 12.0
no service pad (default)
service timestamps debug uptime (default)
service timestamps log uptime (default)
no service password-encryption (default)
hostname Cisco3600
enable secret 8 #7eu2;odg*#,.
ip subnet-zero
no ip 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 20.1.1.1 255.255.255.0
no ip directed-broadcast (default)
ipx network 200
!
interface Serial0
no ip address
no ip directed-broadcast (default)
encapsulation frame-relay
no ip mroutecache (default)
frame-relay lmi-type ansi
```

Sample Cisco 3600 Router Configuration

The following is a sample configuration for the Cisco 3600 router. This configuration is based on performing the tasks in “Configuring the Corporate Router” section on page 3-35. 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` command.

While reviewing the following configuration, also refer to Figure 3-7, which shows the configuration specifics for the Cisco 3600 router.

```plaintext
line vty 0 4
password secret
login
!
end
```
interface Serial0.1 point-to-point
ip address 30.1.1.2 255.255.255.0
no ip directed-broadcast (default)
ipx network AAAA
frame-relay interface-dlci 17

interface Serial0.2 point-to-point
ip address 30.2.1.2 255.255.255.0
no ip directed-broadcast (default)
ipx network BBBB
frame-relay interface-dlci 18

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)

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
Sample Cisco 3600 Router Configuration

Figure 3-7  Sample Cisco 3600 Router Configuration

[Diagram of network setup with labels for DHCP servers, corporate office, serial interface 0, DLCI 17, DLCI 18, subinterfaces, and remote office.]
Configuring Small Office to ISP Networks

This chapter describes how to configure three small-office-to-Internet service provider (ISP) networks, which Table 4-1 presents.

Table 4-1 Sample Networks

<table>
<thead>
<tr>
<th>No.</th>
<th>WAN Options</th>
<th>WAN Encapsulation</th>
<th>Routed Protocols</th>
<th>Other Features</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Synchronous</td>
<td>PPP</td>
<td>IP</td>
<td>Static IP route</td>
<td>• Cisco 805 Fast Step software</td>
</tr>
<tr>
<td></td>
<td>leased line</td>
<td></td>
<td></td>
<td></td>
<td>• CLI</td>
</tr>
<tr>
<td>2</td>
<td>Asynchronous</td>
<td>PPP</td>
<td>IP</td>
<td>Static IP route&lt;br&gt;Easy IP (Phase 1) – Network Address Translation (NAT) and&lt;br&gt;Point-to-Point Protocol/IP Control Protocol (PPP/IPCP)&lt;br&gt;Firewall</td>
<td>• Cisco 805 Fast Step software (template option)&lt;br&gt;• CLI</td>
</tr>
<tr>
<td></td>
<td>dial-up line</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Frame Relay</td>
<td>Frame Relay</td>
<td>IP</td>
<td>Static IP route&lt;br&gt;NAT overload&lt;br&gt;Firewall</td>
<td>• Cisco 805 Fast Step software&lt;br&gt;• CLI</td>
</tr>
</tbody>
</table>

Note Cisco Systems strongly recommends that inexperienced network administrators use the Cisco 805 Fast Step software to configure sample networks 1 and 3. The Cisco 805 Fast Step software might configure the sample networks differently than is described in this guide.
The Cisco 805 Fast Step software is a Windows 95, Windows NT, and Windows 98 based configuration tool included with the Cisco 805 router. For more information, refer to the Cisco 805 Fast Step CD-ROM.

For more information on configuring your router using the CLI, continue reading this chapter.

### Before Configuring Networks

Refer to Table 4-2 to determine what you need to do before configuring each network.

<table>
<thead>
<tr>
<th>Number</th>
<th>WAN Options</th>
<th>What You Must Do</th>
</tr>
</thead>
</table>
| 1      | Leased line, PPP | • Set up IP address scheme.  
         |              | • Buy a range of registered IP addresses for your router Ethernet interface and your LAN devices that require Internet access from the ISP. (If you plan to configure this sample network using the Cisco 805 Fast Step software, you must also buy a registered IP address for your router serial interface.)  
         |              | • Order leased line from your WAN service provider. |
| 2      | Dial-up line, PPP | • Set up IP address scheme.  
         |              | • Ask your ISP to provide the following information:  
         |              | — PPP client name that the ISP assigns as your login name.  
         |              | — PPP password to access your ISP account.  
         |              | — ISP telephone number to dial when you want to establish Internet connection.  
         |              | — PPP authentication protocol used by ISP. (Challenge Handshake Authentication Protocol [CHAP] or Password Authentication Protocol [PAP]¹.)  
         |              | • Buy one registered IP address for router dialer interface.  
         |              | • Order dial-up line from WAN service provider. |
Network 1: Leased Line, PPP

Figure 4-1 shows a sample small office network connected to an ISP with a synchronous leased line. This sample network uses IP as the only routed protocol. Instead of using a dynamic routing protocol such as RIP to learn the route to the ISP, this network uses a static IP route, which is a user-defined route to the ISP.

This network uses registered IP addresses on the router Ethernet interface and on the LAN devices that require Internet access. (You can buy a range of registered IP addresses from your ISP.) To save the cost of buying a registered IP address for the router serial interface, this interface uses the IP address assigned to the Ethernet interface. (If you configure this sample network using the Cisco 805 Fast Step software, you must buy a registered IP address for the router serial interface.)

Table 4-2 Before Configuring Networks (continued)

<table>
<thead>
<tr>
<th>Number</th>
<th>WAN Options</th>
<th>What You Must Do</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Frame Relay</td>
<td>• Set up IP address scheme.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Do the following with the ISP:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>— Buy one registered IP address for router serial interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>— Ask ISP to provide IP address and subnet mask of ISP serial interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Do the following with the WAN service provider:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>— Order one PVC.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>— Ask WAN service provider to provide LMI type.</td>
</tr>
</tbody>
</table>

1 For more information on CHAP and PAP, refer to Appendix C, “Concepts.”
Configuring the Cisco 805 Router

To configure the features for this sample network, perform the tasks described in the following sections on a PC. A sample configuration file 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, refer to the “Entering Global Configuration Mode” section in Chapter 2, “Cisco IOS Basic Skills.” For more information on the commands used in the following tables, refer to the Cisco IOS Release 12.0 documentation set.
## Configuring the Cisco 805 Router

### Global Parameters

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode.</td>
<td>Router#</td>
<td>configure terminal</td>
</tr>
<tr>
<td>2</td>
<td>Specify name for router.</td>
<td>Router (config)#</td>
<td>hostname name</td>
</tr>
<tr>
<td>3</td>
<td>Specify encrypted password to prevent unauthorized access to router.</td>
<td>Router (config)#</td>
<td>enable secret &lt;password&gt;</td>
</tr>
<tr>
<td>4</td>
<td>Configure router to recognize zero subnet range as valid range of addresses.</td>
<td>Router (config)#</td>
<td>ip subnet-zero</td>
</tr>
<tr>
<td>5</td>
<td>Disable router from translating unfamiliar words (typos) entered during a console session into IP addresses.</td>
<td>Router (config)#</td>
<td>no ip domain-lookup</td>
</tr>
</tbody>
</table>

### Ethernet Interface

Use the following table to configure the Ethernet interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode for Ethernet interface.</td>
<td>Router (config)#</td>
<td>interface ethernet 0</td>
</tr>
<tr>
<td>2</td>
<td>Set IP address and subnet mask.</td>
<td>Router (config-if)#</td>
<td>ip address ip-address mask</td>
</tr>
<tr>
<td>3</td>
<td>Enable interface and configuration changes just made to interface.</td>
<td>Router (config-if)#</td>
<td>no shutdown</td>
</tr>
<tr>
<td>4</td>
<td>Exit configuration mode for Ethernet interface.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
</tbody>
</table>
Network 1: Leased Line, PPP

Serial Interface

Use the following table to configure the serial interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode for serial interface.</td>
<td>Router (config)#</td>
<td>interface serial 0</td>
</tr>
<tr>
<td>2</td>
<td>Set IP address to address used on Ethernet interface.</td>
<td>Router (config-if)#</td>
<td>ip unnumbered ethernet 0</td>
</tr>
<tr>
<td>3</td>
<td>Specify PPP as encapsulation (framing) method.</td>
<td>Router (config-if)#</td>
<td>encapsulation ppp</td>
</tr>
<tr>
<td>4</td>
<td>Enable interface and configuration changes just made to interface.</td>
<td>Router (config-if)#</td>
<td>no shutdown</td>
</tr>
<tr>
<td>5</td>
<td>Exit configuration mode for serial interface.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
<tr>
<td>6</td>
<td>Set up a static route to ISP router.</td>
<td>Router (config)#</td>
<td>ip route 0.0.0.0 0.0.0.0 serial 0</td>
</tr>
</tbody>
</table>

Command-Line Access to the Router

Use the following table to configure parameters to control access to the router.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter line configuration mode, and specify the console terminal line.</td>
<td>Router (config)#</td>
<td>line console 0</td>
</tr>
<tr>
<td>2</td>
<td>Specify a unique password on the line.</td>
<td>Router (config-line)#</td>
<td>password &lt;password&gt;</td>
</tr>
<tr>
<td>3</td>
<td>Enable password checking at terminal session login.</td>
<td>Router (config-line)#</td>
<td>login</td>
</tr>
<tr>
<td>4</td>
<td>Specify a virtual terminal for remote console access.</td>
<td>Router (config-line)#</td>
<td>line vty 0 4</td>
</tr>
<tr>
<td>5</td>
<td>Specify a unique password on the line.</td>
<td>Router (config-line)#</td>
<td>password &lt;password&gt;</td>
</tr>
</tbody>
</table>
Sample Configuration

The following is a sample configuration based on performing the tasks in “Configuring the Cisco 805 Router” section on page 4-4. 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` command.

```
Current configuration:
!
version 12.0
no service pad (default)
service timestamps debug uptime (default)
service timestamps log uptime (default)
no service password-encryption (default)
hostname Cisco805
enable secret 5 $1$RnI.$K4mh5q4MFetaqKzBbQ7gv0
ip subnet-zero
no ip domain-lookup
!
interface Ethernet0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast (default)
!
interface Serial0
ip unnumbered ethernet 0
no ip directed-broadcast (default)
encapsulation ppp
!
no ip http server (default)
ip classless (default)
!
ip route 0.0.0.0 0.0.0.0 serial 0
!
line con 0
exec-timeout 10 0 (default)
```

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Enable password checking at virtual terminal session login.</td>
<td>Router (config-line)#</td>
<td>login</td>
</tr>
<tr>
<td>7</td>
<td>Exit line configuration mode, and return to privileged EXEC mode.</td>
<td>Router (config-line)#</td>
<td>end</td>
</tr>
</tbody>
</table>

Sample Configuration

The following is a sample configuration based on performing the tasks in “Configuring the Cisco 805 Router” section on page 4-4. 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` command.

```
Current configuration:
!
version 12.0
no service pad (default)
service timestamps debug uptime (default)
service timestamps log uptime (default)
no service password-encryption (default)
hostname Cisco805
enable secret 5 $1$RnI.$K4mh5q4MFetaqKzBbQ7gv0
ip subnet-zero
no ip domain-lookup
!
interface Ethernet0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast (default)
!
interface Serial0
ip unnumbered ethernet 0
no ip directed-broadcast (default)
encapsulation ppp
!
no ip http server (default)
ip classless (default)
!
ip route 0.0.0.0 0.0.0.0 serial 0
!
line con 0
exec-timeout 10 0 (default)
```

Sample Configuration

The following is a sample configuration based on performing the tasks in “Configuring the Cisco 805 Router” section on page 4-4. 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` command.

```
Current configuration:
!
version 12.0
no service pad (default)
service timestamps debug uptime (default)
service timestamps log uptime (default)
no service password-encryption (default)
hostname Cisco805
enable secret 5 $1$RnI.$K4mh5q4MFetaqKzBbQ7gv0
ip subnet-zero
no ip domain-lookup
!
interface Ethernet0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast (default)
!
interface Serial0
ip unnumbered ethernet 0
no ip directed-broadcast (default)
encapsulation ppp
!
no ip http server (default)
ip classless (default)
!
ip route 0.0.0.0 0.0.0.0 serial 0
!
line con 0
exec-timeout 10 0 (default)
```
Network 2: Dial-up Line, PPP

password 4youreyesonly
login
transport input none (default)
stopbits 1 (default)
line vty 0 4
password secret
login
!
end

Network 2: Dial-up Line, PPP

Figure 4-2 shows a sample small office network connected to an ISP with a asynchronous dial-up line running PPP. This sample network uses IP as the only routed protocol. Instead of using a dynamic routing protocol such as RIP to learn the route to the ISP, this network uses a static IP route, which is a user-defined route to the ISP.

This sample network uses the dial-on-demand routing (DDR) implementation of dialer profiles. For conceptual information, refer to the “Dialer Profiles” section in Appendix C, “Concepts.”

This sample network uses nonregistered IP addresses on the router Ethernet interface and the LAN devices. To solve the problem of using nonregistered IP addresses when accessing the Internet, this sample network uses Easy IP (Phase 1). This feature combines NAT and PPP/IPCP. With this feature, the Cisco 805 router can automatically negotiate a registered IP address for the router dialer interface from the ISP router. All devices in this sample network can use this registered IP address when accessing the Internet. For more information on this feature, including configuration information, refer to the “Configuring Easy IP (Phase 1)” section in Chapter 5, “Advanced Features.”

You can also configure the firewall feature in this sample network.
Configuring the Cisco 805 Router

To configure the features for this sample network, perform the tasks described in the following sections on a PC. A sample configuration file 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, refer to the “Entering Global Configuration Mode” section in Chapter 2, “Cisco IOS Basic Skills.” For more information on the commands used in the following tables, refer to the Cisco IOS Release 12.0 documentation set.
Global Parameters

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode.</td>
<td>Router#</td>
<td>configure terminal</td>
</tr>
<tr>
<td>2</td>
<td>Specify name for router.</td>
<td>Router (config)#</td>
<td>hostname name</td>
</tr>
<tr>
<td>3</td>
<td>Specify encrypted password to prevent unauthorized access to router.</td>
<td>Router (config)#</td>
<td>enable secret &lt;password&gt;</td>
</tr>
<tr>
<td>4</td>
<td>Configure router to recognize zero subnet range as valid range of addresses.</td>
<td>Router (config)#</td>
<td>ip subnet-zero</td>
</tr>
<tr>
<td>5</td>
<td>Disable router from translating unfamiliar words (typos) entered during a console session into IP addresses.</td>
<td>Router (config)#</td>
<td>no ip domain-lookup</td>
</tr>
</tbody>
</table>

Ethernet Interface

Use the following table to configure the Ethernet interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode for Ethernet interface.</td>
<td>Router (config)#</td>
<td>interface ethernet 0</td>
</tr>
<tr>
<td>2</td>
<td>Set IP address and subnet mask.</td>
<td>Router (config-if)#</td>
<td>ip address ip-address mask</td>
</tr>
<tr>
<td>3</td>
<td>Enable interface and configuration changes just made to interface.</td>
<td>Router (config-if)#</td>
<td>no shutdown</td>
</tr>
<tr>
<td>4</td>
<td>Exit configuration mode for Ethernet interface.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
</tbody>
</table>
Configuring the Cisco 805 Router

Serial Interface

Use the following table to configure the serial interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode for serial interface.</td>
<td>Router (config)#</td>
<td><code>interface serial 0</code></td>
</tr>
<tr>
<td>2</td>
<td>Remove any IP address associated with serial interface.</td>
<td>Router (config-if)#</td>
<td><code>no ip address</code></td>
</tr>
<tr>
<td>3</td>
<td>Specify PPP as encapsulation (framing) type.</td>
<td>Router (config-if)#</td>
<td><code>encapsulation ppp</code></td>
</tr>
<tr>
<td>4</td>
<td>Enable CHAP and/or PAP, and specify authentication on incoming (received) calls only.</td>
<td>Router (config-if)#</td>
<td><code>ppp authentication chap pap callin</code> or <code>ppp authentication chap callin</code> or <code>ppp authentication pap callin</code></td>
</tr>
<tr>
<td>5</td>
<td>Specify mode of serial interface as asynchronous.</td>
<td>Router (config-if)#</td>
<td><code>physical-layer async</code></td>
</tr>
<tr>
<td>6</td>
<td>Configure asynchronous line for data traffic.</td>
<td>Router (config-if)#</td>
<td><code>async mode dedicated</code></td>
</tr>
<tr>
<td>7</td>
<td>Specify that you are using DDR.</td>
<td>Router (config-if)#</td>
<td><code>dialer in-band</code></td>
</tr>
<tr>
<td>8</td>
<td>Set up dialer pool, and assign serial interface to the dialer pool.</td>
<td>Router (config-if)#</td>
<td><code>dialer pool-member number</code></td>
</tr>
<tr>
<td>9</td>
<td>Enable interface and configuration changes just made to interface.</td>
<td>Router (config-if)#</td>
<td><code>no shutdown</code></td>
</tr>
<tr>
<td>10</td>
<td>Exit serial configuration mode.</td>
<td>Router (config-if)#</td>
<td><code>exit</code></td>
</tr>
</tbody>
</table>

Dialer Profile

To configure the dialer profile, you must set up a dialer interface and dialer pool. (Dialer pools are set up with the serial interface.) For conceptual information, refer to the “Dialer Profiles” section in Appendix C, “Concepts.”

Use the following table to configure the dialer interface.
### Network 2: Dial-up Line, PPP

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode for and define dialer rotary group.</td>
<td>Router (config)#</td>
<td>interface dialer 1</td>
</tr>
<tr>
<td>2</td>
<td>Specify PPP as encapsulation (framing) type.</td>
<td>Router (config-if)#</td>
<td>encapsulation ppp</td>
</tr>
<tr>
<td>3</td>
<td>Specify ISP router authentication name.</td>
<td>Router (config-if)#</td>
<td>dialer remote-name name</td>
</tr>
<tr>
<td>4</td>
<td>Specify amount of idle time before calls are disconnected.</td>
<td>Router (config-if)#</td>
<td>dialer idle-timeout seconds either</td>
</tr>
<tr>
<td>5</td>
<td>Specify telephone number of ISP router.</td>
<td>Router (config-if)#</td>
<td>dialer string string modem-script chat-script-name</td>
</tr>
<tr>
<td>6</td>
<td>Specify dialer pool to use for calls to ISP. (Dialer pool was set up in “Serial Interface” section on page 4-11.)</td>
<td>Router (config-if)#</td>
<td>dialer pool number</td>
</tr>
<tr>
<td>7</td>
<td>Assign dialer interface to a dialer group.</td>
<td>Router (config-if)#</td>
<td>dialer-group number</td>
</tr>
<tr>
<td>8</td>
<td>Enable CHAP and/or PAP, and specify authentication on incoming (received) calls only.</td>
<td>Router (config-if)#</td>
<td>ppp authentication chap pap callin or ppp authentication chap callin or ppp authentication pap callin</td>
</tr>
<tr>
<td>9</td>
<td>Set up CHAP hostname and password.</td>
<td>Router (config-if)#</td>
<td>ppp chap hostname hostname ppp chap password &lt;secret&gt;</td>
</tr>
<tr>
<td>10</td>
<td>Set up PAP username and password.</td>
<td>Router (config-if)#</td>
<td>ppp pap sent-username username password &lt;password&gt;</td>
</tr>
<tr>
<td>11</td>
<td>Disable CDP.</td>
<td>Router (config-if)#</td>
<td>no cdp enable</td>
</tr>
<tr>
<td>12</td>
<td>Enable interface and configuration changes just made to interface.</td>
<td>Router (config-if)#</td>
<td>no shutdown</td>
</tr>
<tr>
<td>13</td>
<td>Exit configuration mode for dialer interface.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
<tr>
<td>14</td>
<td>Set up static route to ISP router.</td>
<td>Router (config)#</td>
<td>ip route 0.0.0.0 0.0.0.0 dialer 1</td>
</tr>
</tbody>
</table>

4-12 Cisco 805 Router Software Configuration Guide
For information on controlling the types of traffic that can activate your dial-up line and increase your monthly dial-up line cost, refer to the “Controlling Dial-up Line Activation” section in Chapter 5, “Advanced Features.”

Asynchronous Line

Use the following table to configure the asynchronous line.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode for asynchronous</td>
<td>Router (config)#</td>
<td>line 1</td>
</tr>
<tr>
<td></td>
<td>line (line 1).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Specifies that router should send and listen</td>
<td>Router (config-line) #</td>
<td>flowcontrol hardware</td>
</tr>
<tr>
<td></td>
<td>to flow control information from attached</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>serial device.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Specify that all protocols can connect to</td>
<td>Router (config-line) #</td>
<td>transport input all</td>
</tr>
<tr>
<td></td>
<td>line 1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Configure line 1 for both incoming and</td>
<td>Router (config-line) #</td>
<td>modem inout</td>
</tr>
<tr>
<td></td>
<td>outgoing calls.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Set baud rate.</td>
<td>Router (config-line) #</td>
<td>speed 115200</td>
</tr>
<tr>
<td>6</td>
<td>Set stop bits.</td>
<td>Router (config-line) #</td>
<td>stopbits 1</td>
</tr>
<tr>
<td>7</td>
<td>Exit configuration mode for serial interface.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
</tbody>
</table>
Easy IP (Phase 1)

For information on configuring Easy IP (Phase 1), refer to the “Configuring Easy IP (Phase 1)” section in Chapter 5, “Advanced Features.”

Firewall Feature

For information on configuring a firewall, refer to the *Cisco IOS Firewall Feature Set* feature module, which appears on Cisco Connection Online (CCO) only.

Command-Line Access to the Router

Use the following table to configure parameters to control access to the router.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter line configuration mode, and specify the console terminal line.</td>
<td>Router (config)#</td>
<td>line console 0</td>
</tr>
<tr>
<td>2</td>
<td>Specify a unique password on the line.</td>
<td>Router (config-line)#</td>
<td>password &lt;password&gt;</td>
</tr>
<tr>
<td>3</td>
<td>Enable password checking at terminal session login.</td>
<td>Router (config-line)#</td>
<td>login</td>
</tr>
<tr>
<td>4</td>
<td>Specify a virtual terminal for remote console access.</td>
<td>Router (config-line)#</td>
<td>line vty 0 4</td>
</tr>
<tr>
<td>5</td>
<td>Specify a unique password on the line.</td>
<td>Router (config-line)#</td>
<td>password &lt;password&gt;</td>
</tr>
<tr>
<td>6</td>
<td>Enable password checking at virtual terminal session login.</td>
<td>Router (config-line)#</td>
<td>login</td>
</tr>
<tr>
<td>7</td>
<td>Exit line configuration mode, and return to privileged EXEC mode.</td>
<td>Router (config-line)#</td>
<td>end</td>
</tr>
</tbody>
</table>

Sample Configuration

The following is a sample configuration based on performing the tasks in “Configuring the Cisco 805 Router” section on page 4-9. It does not show firewall-related commands. For a sample configuration of the firewall feature, refer to the *Cisco IOS Firewall Feature Set* feature module, which appears on Cisco Connection Online (CCO) only.
Sample 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` command.

```
Current configuration:
!
version 12.0
no service pad (default)
no service password-encryption (default)
no service pad (default)
service timestamps debug uptime (default)
service timestamps log uptime (default)
hostname Cisco805
enable secret 5 $1$RnI.$K4mh5q4MFetaqKzBbq7gv0
ip subnet-zero
no ip domain-lookup
chat-script dial "" AT OK "\patdt\T" TIMEOUT 60 CONNECT \C
!This generic chat script is known to work. For information on
!customizing your chat script, refer to the Dial Solutions Configuration
!Guide.
!
interface Ethernet0
ip address 10.1.1.1 255.255.255.0
no ip directed-broadcast (default)
no ip directed-broadcast (default)
!
interface Serial0
physical-layer async
no ip address
no ip directed-broadcast (default)
encapsulation ppp
dialer in-band
dialer pool-member 1
async mode dedicated
ppp authentication chap pap callin
ppp chap hostname chapisp
ppp chap password abra
ppp pap sent-username papisp password cadabra
!
interface Dialer1
ip address negotiated
no ip directed-broadcast (default)
encapsulation ppp
dialer remote-name isp
dialer idle-timeout 500
dialer string 5551111 modem-script dial
```
Network 3: Frame Relay

dialer pool 1
dialer-group 1
no cdp enable
ppp authentication chap pap callin
ppp chap hostname chapisp
ppp chap password abra
ppp pap sent-username papisp password cadabra
ip nat outside
!
no ip http server (default)
ip classless (default)
!
ip route 0.0.0.0 0.0.0.0 dialer 1
dialer-list 1 protocol ip permit
ip nat inside source list 1 interface dialer 0 overload
access-list 1 permit 10.0.0.0 0.255.255.255
!
line con 0
exec-timeout 10 0 (default)
password 4youreyesonly
login
transport input none (default)
stopbits 1 (default)
line 1
modem InOut
transport input all
speed 115200
flowcontrol hardware
line vty 0 4
password secret
login
!
end

Network 3: Frame Relay

Figure 4-3 shows a sample small office network connected to an ISP with Frame Relay. This sample network uses IP as the only routed protocol. Instead of using a dynamic routing protocol such as RIP to learn the route to the ISP, this network uses a static IP route, which is a user-defined route to the ISP.
This sample network uses nonregistered IP addresses on the router Ethernet interface and the LAN devices. To solve the problem of using nonregistered IP addresses when accessing the Internet, this sample network uses the NAT overload feature. You buy one registered IP address for the serial interface from the ISP, then using NAT overload, all devices in this sample network can use this registered IP address when accessing the Internet. For more information on this feature, including configuration information, refer to the “Configuring NAT Overload” section in Chapter 5, “Advanced Features.”

You can also configure the firewall feature in this sample network.

**Figure 4-3 Network 3**

Network address:
IP: 10.0.0.0

---

**Configuring the Cisco 805 Router**

To configure the features for this sample network, perform the tasks described in the following sections on a PC. A sample configuration file 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, refer to the “Entering Global Configuration Mode” section in Chapter 2, “Cisco IOS Basic Skills.” For more information on the commands used in the following tables, refer to the Cisco IOS Release 12.0 documentation set.
### Global Parameters

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode.</td>
<td>Router#</td>
<td>configure terminal</td>
</tr>
<tr>
<td>2</td>
<td>Specify name for router.</td>
<td>Router (config)#</td>
<td>hostname name</td>
</tr>
<tr>
<td>3</td>
<td>Specify encrypted password to prevent unauthorized access to router.</td>
<td>Router (config)#</td>
<td>enable secret &lt;password&gt;</td>
</tr>
<tr>
<td>4</td>
<td>Configure router to recognize zero subnet range as valid range of addresses.</td>
<td>Router (config)#</td>
<td>ip subnet-zero</td>
</tr>
<tr>
<td>5</td>
<td>Disable router from translating unfamiliar words (typos) entered during a console session into IP addresses.</td>
<td>Router (config)#</td>
<td>no ip domain-lookup</td>
</tr>
</tbody>
</table>

### Ethernet Interface

Use the following table to configure the Ethernet interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode for Ethernet interface.</td>
<td>Router (config)#</td>
<td>interface ethernet 0</td>
</tr>
<tr>
<td>2</td>
<td>Set IP address and subnet mask.</td>
<td>Router (config-if)#</td>
<td>ip address ip-address mask</td>
</tr>
<tr>
<td>3</td>
<td>Enable interface and configuration changes just made to interface.</td>
<td>Router (config-if)#</td>
<td>no shutdown</td>
</tr>
<tr>
<td>4</td>
<td>Exit configuration mode for Ethernet interface.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
</tbody>
</table>
Configuring the Cisco 805 Router

Serial Interface

Use the following table to configure the serial interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode for serial interface.</td>
<td>Router (config)#</td>
<td>interface serial 0</td>
</tr>
<tr>
<td>2</td>
<td>Set IP address and subnet mask.</td>
<td>Router (config-if)#</td>
<td>ip address ip-address mask</td>
</tr>
<tr>
<td>4</td>
<td>Set encapsulation (framing) method to Frame Relay. If the ISP router is not a Cisco router, use ietf option.</td>
<td>Router (config-if)#</td>
<td>encapsulation frame relay [ietf]</td>
</tr>
<tr>
<td>5</td>
<td>Set LMI type to type provided by Frame Relay service provider. (Default is cisco.)</td>
<td>Router (config-if)#</td>
<td>frame-relay lmi-type {ansi</td>
</tr>
<tr>
<td>6</td>
<td>Enable interface and configuration changes just made to interface.</td>
<td>Router (config-if)#</td>
<td>no shutdown</td>
</tr>
<tr>
<td>7</td>
<td>Exit configuration mode for serial interface.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
<tr>
<td>8</td>
<td>Set up a static route to ISP router.</td>
<td>Router (config)#</td>
<td>ip route 0.0.0.0 0.0.0.0 serial 0</td>
</tr>
</tbody>
</table>

NAT Overload

For information on configuring NAT overload, refer to the “Configuring NAT Overload” section in Chapter 5, “Advanced Features.”

Firewall Feature

For information on configuring a firewall, refer to the *Cisco IOS Firewall Feature Set* feature module, which appears on Cisco Connection Online (CCO) only.
Command-Line Access to the Router

Use the following table to configure parameters to control access to the router.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter line configuration mode, and specify the</td>
<td>Router (config)#</td>
<td>line console 0</td>
</tr>
<tr>
<td></td>
<td>console terminal line.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Specify a unique password on the line.</td>
<td>Router (config-line)#</td>
<td>password &lt;password&gt;</td>
</tr>
<tr>
<td>3</td>
<td>Enable password checking at terminal session</td>
<td>Router (config-line)#</td>
<td>login</td>
</tr>
<tr>
<td></td>
<td>login.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Specify a virtual terminal for remote console</td>
<td>Router (config-line)#</td>
<td>line vty 0 4</td>
</tr>
<tr>
<td></td>
<td>access.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Specify a unique password on the line.</td>
<td>Router (config-line)#</td>
<td>password &lt;password&gt;</td>
</tr>
<tr>
<td>6</td>
<td>Enable password checking at virtual terminal</td>
<td>Router (config-line)#</td>
<td>login</td>
</tr>
<tr>
<td></td>
<td>session login.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Exit line configuration mode, and return to</td>
<td>Router (config-line)#</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>privileged EXEC mode.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Sample Configuration

The following is a sample configuration based on performing the tasks in “Configuring the Cisco 805 Router” section on page 4-17. 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` command.
Sample Configuration

Current configuration:
!
version 12.0
no service pad (default)
service timestamps debug uptime (default)
service timestamps log uptime (default)
no service password-encryption (default)
hostname Cisco805
enable secret 5 $1$Rn1.$K4mh5q4MFetaqKzBbQ7gv0
ip subnet-zero
no ip domain-lookup
!
interface Ethernet0
ip address 10.1.1.1 255.255.255.0
no ip directed-broadcast (default)
ip nat inside
!
interface Serial0
ip address 192.168.0.2 255.255.255.0
no ip directed-broadcast (default)
no ip mroute-cache (default)
encapsulation frame-relay ietf
frame-relay lmi-type ansi
ip nat outside
!
no ip http server (default)
ip classless (default)
!
ip route 0.0.0.0 0.0.0.0 serial 0
ip nat inside source list 1 interface serial 0 overload
access-list 1 permit 10.0.0.0 0.255.255.255
!
line con 0
exec-timeout 10 0 (default)
password 4youreyesonly
login
transport input none (default)
stopbits 1 (default)
line vty 0 4
password secret
login
!
end
Advanced Features

This chapter contains information on the following advanced features, which can be set up in the specified sample remote-office-to-corporate-office or small-office-to-ISP networks:

- IP Enhanced Interior Gateway Routing Protocol (EIGRP)
- Easy IP (Phase 1)
- Easy IP (Phase 2)
- Network Address Translation (NAT) overload
- Firewall
- Windows NT (configuring Cisco 805 router to function in a Windows NT environment)
- Dial-up line activation control
- IP network access restriction
Configuring IP EIGRP

This section explains how to configure IP EIGRP in Network 1: Leased Line, HDLC, Network 2: Leased Line, PPP, Network 3: X.25, and Network 5: Frame Relay. Each of these sample networks is presented in Chapter 3, “Configuring Remote Office to Corporate Office Networks.”

Use the following table to configure IP EIGRP. For information on the commands used in this table, refer to the Cisco IOS Release 12.0 documentation set.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode</td>
<td>Router#</td>
<td>configure terminal</td>
</tr>
<tr>
<td>2</td>
<td>Enter router configuration mode, and enable EIGRP.</td>
<td>Router (config)#</td>
<td>router eigrp autonomous-system</td>
</tr>
<tr>
<td>3</td>
<td>Specify this command for each directly connected network.</td>
<td>Router (config-router)#</td>
<td>network network-number</td>
</tr>
<tr>
<td>4</td>
<td>Exit router configuration mode.</td>
<td>Router (config-router)#</td>
<td>exit</td>
</tr>
</tbody>
</table>

Configuring Easy IP (Phase 1)

This section explains how to configure Easy IP (Phase 1) in Network 2: Dial-up Line, PPP in Chapter 4, “Configuring Small Office to ISP Networks.”

The Easy IP (Phase 1) feature combines NAT and PPP/Internet Protocol Control Protocol (IPCP). With PPP/IPCP, the Cisco 805 router automatically negotiates a globally unique (registered) IP address for the dialer interface from the ISP router. 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 for 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).

Use the following table to configure Easy IP (Phase 1). For information on the commands used in this table, refer to the Cisco IOS Release 12.0 documentation set.
Configuring Easy IP (Phase 1)

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode.</td>
<td>Router#</td>
<td>configure terminal</td>
</tr>
<tr>
<td>2</td>
<td>Define standard access list that permits nonregistered IP addresses of hosts.</td>
<td>Router (config)#</td>
<td>access-list access-list-number permit source [source-wildcard]</td>
</tr>
<tr>
<td>3</td>
<td>Set up translation of addresses identified by previously defined access list.</td>
<td>Router (config)#</td>
<td>ip nat inside source list access-list-number interface interface overload</td>
</tr>
<tr>
<td>4</td>
<td>Enter configuration mode for Ethernet interface.</td>
<td>Router (config)#</td>
<td>interface ethernet 0</td>
</tr>
<tr>
<td>5</td>
<td>Establish Ethernet interface as inside interface for NAT.</td>
<td>Router (config-if)#</td>
<td>ip nat inside</td>
</tr>
<tr>
<td>6</td>
<td>Enable interface and configuration changes just made to interface.</td>
<td>Router (config-if)#</td>
<td>no shutdown</td>
</tr>
<tr>
<td>7</td>
<td>Exit configuration mode for Ethernet interface.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
<tr>
<td>8</td>
<td>Enter configuration mode for dialer interface.</td>
<td>Router (config)#</td>
<td>interface dialer-name</td>
</tr>
<tr>
<td>9</td>
<td>Enable PPP/IPCP to automatically negotiate globally unique IP address from ISP router.</td>
<td>Router (config-if)#</td>
<td>ip address negotiated</td>
</tr>
<tr>
<td>10</td>
<td>Establish dialer interface as outside interface for NAT.</td>
<td>Router (config-if)#</td>
<td>ip nat outside</td>
</tr>
<tr>
<td>11</td>
<td>Enable interface and configuration changes just made to interface.</td>
<td>Router (config-if)#</td>
<td>no shutdown</td>
</tr>
<tr>
<td>12</td>
<td>Exit configuration mode for serial interface.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
</tbody>
</table>
The following is a sample configuration file that contains commands relevant to Easy IP (Phase 1) only:

```
! interface ethernet 0
 ip address 10.1.1.2 255.255.255.0
 ip nat inside
!
 ! interface dialer 0
 ip address negotiated
 ip nat outside
!
 ip nat inside source list 1 interface dialer 0 overload
 access list 1 permit 10.0.0.0 0.255.255.255
!
```

This sample configuration file does the following (refer to Figure 5-1):

- Enables packets having the source address of 10.0.0.0 to 10.255.255.255 to be translated to the globally unique IP address assigned to the router dialer interface and vice versa. The router retains TCP and UDP port numbers of each inside host to translate the global IP address back to the correct local address.

- Establishes the Ethernet interface as an inside interface for NAT.

- Enables PPP/IPCP to automatically negotiate a globally unique IP address for the router dialer interface from the ISP router.

- Establishes the dialer interface as an outside interface for NAT.
Configuring Easy IP (Phase 1)

For example, if host A attempts to open a connection to host C, the following events occur:

- If the Cisco 805 router does not already have a global IP address for the dialer interface, it requests one from the ISP router.
- The ISP router responds with the global IP address of 172.16.0.1.
- The Cisco 805 router creates a translation that associates the global IP address of the dialer interface (172.16.0.1) with the nonregistered IP address of host A (10.1.1.2). NAT uses the TCP and UDP ports to associate the nonregistered IP address to the global IP address.
- The Cisco 805 router forwards the packet to host C.
When host C attempts to respond to host A, the Cisco 805 router determines that the global IP address 172.16.0.1 contained in the packet for host A should be translated back to 10.1.1.2. Specifically, the router looks at the inside global IP address and TCP port number (172.16.0.1:1723) in the NAT table and searches for the same TCP port number in the inside local IP address and TCP port number (10.1.1.2:1723).

Configuring Easy IP (Phase 2)

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 or PC or a Cisco router. This section explains how to configure the Cisco 805 router as a DHCP server.

With the DHCP relay feature configured on the Cisco 805 router, this router can relay IP address requests from the LAN interface, over the serial or dialer interface, and to the DHCP server as shown in Figure 5-2.

Figure 5-2  Easy IP (Phase 2) – DHCP Server and Relay

This section explains how to configure the following:

- DHCP server in Network 4: Dial-up Line, PPP in Chapter 3, “Configuring Remote Office to Corporate Office Networks.”
- DHCP relay in Network 5: Frame Relay in Chapter 3, “Configuring Remote Office to Corporate Office Networks.”
DHCP Server

Use the following table to configure the Cisco 805 router as a DHCP server. For information on the commands used in this table, refer to the Cisco IOS Release 12.0 documentation set.

**Note** This configuration uses a subset of existing DHCP server features. For more information on the features not used in this configuration, refer to the *Cisco IOS DHCP Server* feature module.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode.</td>
<td>Router#</td>
<td>configure terminal</td>
</tr>
<tr>
<td>2</td>
<td>Enter DHCP configuration mode, and create pool of IP addresses that can be assigned to DHCP clients.</td>
<td>Router (config)#</td>
<td>ip dhcp pool name</td>
</tr>
<tr>
<td>3</td>
<td>Specify range of IP addresses that can be assigned.</td>
<td>Router (dhcp-config)#</td>
<td>network ip-address subnet-mask</td>
</tr>
<tr>
<td>4</td>
<td>Designate router as default router, and specify IP address.</td>
<td>Router (dhcp-config)#</td>
<td>default-router ip-address</td>
</tr>
<tr>
<td>5</td>
<td>Exit DHCP configuration mode.</td>
<td>Router (dhcp-config)#</td>
<td>exit</td>
</tr>
</tbody>
</table>

The following is a sample configuration file that contains commands relevant to DHCP server only:

```
!
ip dhcp pool dhcppool_1
network 10.1.1.1 255.255.255.0
default-router 10.1.1.1
!```
This sample configuration does the following (refer to Figure 5-3):

- Creates a pool (dhcppool_1) of 254 reusable IP addresses (10.1.1.1 to 10.1.1.254) that can be assigned.
- Designates the Cisco 805 router as the DHCP server to which DHCP clients send their IP address requests and assigns the IP address of 10.1.1.1 to the router.

The first DHCP client to request an IP address is assigned 10.1.1.2 and so on until a client is assigned 10.1.1.254. After the range of 254 IP addresses is assigned, the DHCP server reassigns 10.1.1.2 and so on.

**DHCP Relay**

DHCP relay configures the router to forward UDP broadcasts, including IP address requests, from DHCP clients. However, if your network uses a dial-up line, you might find that this line is activated excessively because of the IP address requests and other UDP broadcasts. If keeping monthly dial-up costs low is a concern, you can control the activation of your dial-up line. For more information, refer to the “Controlling Dial-up Line Activation” section later in this chapter.
Use the steps in this table to configure DHCP relay on the Cisco 805 router. For information on the commands used in this table, refer to the Cisco IOS Release 12.0 documentation set.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode.</td>
<td>Router#</td>
<td>configure terminal</td>
</tr>
<tr>
<td>2</td>
<td>Specify which DHCP server to use on your network.</td>
<td>Router (config)#</td>
<td>ip dhcp-server ip-address</td>
</tr>
<tr>
<td>3</td>
<td>Enter configuration mode for serial interface.</td>
<td>Router (config)#</td>
<td>interface serial 0</td>
</tr>
<tr>
<td>4</td>
<td>Forward default UDP broadcasts including IP configuration requests to the DHCP server.</td>
<td>Router (config-if)#</td>
<td>ip helper-address address</td>
</tr>
<tr>
<td>5</td>
<td>Enable interface and configuration changes just made to interface.</td>
<td>Router (config-if)#</td>
<td>no shutdown</td>
</tr>
<tr>
<td>6</td>
<td>Exit configuration mode for serial interface.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
</tbody>
</table>

The following is a sample configuration file that contains commands relevant to DHCP relay only:

```
!  ip dhcp-server 10.1.1.1 !
!  interface serial 0
!  ip helper-address 10.1.1.1 !
```

This sample configuration does the following (refer to Figure 5-4):

- Designates the DHCP server.
- Configures the Cisco 805 router to forward UDP broadcasts, including IP address requests, from DHCP clients to the DHCP server.
Configuring NAT Overload

This section explains how to configure NAT overload in Network 3: Frame Relay in Chapter 4, “Configuring Small Office to ISP Networks.”

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 address (the nonregistered IP address assigned to a host on the inside network) to a globally unique IP address before sending packets to the outside network.

Use the following table to configure NAT overload. For information on the commands used in this table, refer to the Cisco IOS Release 12.0 documentation set.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode.</td>
<td>Router#</td>
<td>configure terminal</td>
</tr>
<tr>
<td>2</td>
<td>Define a standard access list.</td>
<td>Router (config)#</td>
<td>access-list access-list-number permit source [source-wildcard]</td>
</tr>
<tr>
<td>3</td>
<td>Establish static source translation, identifying access list defined in previous step.</td>
<td>Router (config)#</td>
<td>ip nat inside source list access-list-number interface interface overload</td>
</tr>
<tr>
<td>4</td>
<td>Enter configuration mode for Ethernet interface.</td>
<td>Router (config)#</td>
<td>interface ethernet 0</td>
</tr>
</tbody>
</table>

5-10 Cisco 805 Router Software Configuration Guide
Configuring NAT Overload

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Establish Ethernet interface as inside interface.</td>
<td>Router (config-if)#</td>
<td>ip nat inside</td>
</tr>
<tr>
<td>6</td>
<td>Enable interface and configuration changes just made to interface.</td>
<td>Router (config-if)#</td>
<td>no shutdown</td>
</tr>
<tr>
<td>7</td>
<td>Exit configuration mode for Ethernet interface.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
<tr>
<td>8</td>
<td>Enter configuration mode for serial interface.</td>
<td>Router (config)#</td>
<td>interface serial 0</td>
</tr>
<tr>
<td>9</td>
<td>Establish serial interface as outside interface.</td>
<td>Router (config-if)#</td>
<td>ip nat outside</td>
</tr>
<tr>
<td>10</td>
<td>Enable interface and configuration changes just made to interface.</td>
<td>Router (config-if)#</td>
<td>no shutdown</td>
</tr>
<tr>
<td>11</td>
<td>Exit configuration mode for serial interface.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
</tbody>
</table>

The following is a sample configuration file that contains commands relevant to NAT overload only:

```
!
interface ethernet 0
ip address 10.1.1.2 255.255.255.0
ip nat inside
!
interface serial 0
ip address 172.16.0.1 255.255.255.0
ip nat outside
!
access list 1 permit 10.0.0.0 0.255.255.255
ip nat inside source list 1 interface serial 0 overload
!
```
This sample configuration file does the following (refer to Figure 5-5):

- Enables packets having the source address of 10.0.0.0 to 10.255.255.255 to be translated to the globally unique IP address assigned to the router serial port (172.16.0.1) and vice versa. The router allows multiple local addresses (10.0.0.0 to 10.255.255.255) to use the same globally unique IP address (overloading). The router retains TCP and UDP port numbers of each inside host to translate the global IP address back to the correct local address.

- Establishes the Ethernet interface as an inside interface.
- Establishes the serial interface as an outside interface.

If hosts A and B attempt to open a connection to host C, the router does the following:

- Determines that the IP addresses of host A (10.1.1.2) and host B (10.1.1.3) should be translated to 172.16.0.1.
- Forwards the packets from hosts A and B to host C.
When host C attempts to respond to hosts A and B, the router does the following:

- Determines that the global IP address 172.16.0.1 contained in the respective packets for hosts A and B should be translated back to the correct local addresses.

For example, in the case of the packet for host A, the router looks at the inside global IP address and TCP port number (172.16.0.1:1723) in the NAT table and searches for the same TCP port number in the inside local IP address and TCP port number (10.1.1.2:1723).

Configuring the Firewall Feature

To configure a firewall, you must have one of the Cisco 805 software images that contain the firewall feature. For information on the firewall features that the Cisco 805 router supports, refer to the release notes that ship with the Cisco 805 router.

Small-office-to-ISP networks 2 and 3 (asynchronous dial-up line with PPP and Frame Relay, respectively) use the firewall feature to block undesired traffic from the ISP. To configure a firewall in these sample networks, you can use either the Cisco 805 Fast Step software (recommended for inexperienced network administrators) or the Cisco IOS software command-line interface (CLI) (recommended for more experienced network administrators).

For information on how to use the Cisco 805 Fast Step application, refer to the application online help. For information on how to configure a firewall using the CLI, refer to the Cisco IOS Firewall Feature Set feature module, which appears on Cisco Connection Online (CCO) only. This feature module also provides conceptual information on the firewall feature.

**Note** The Cisco 805 Fast Step software might configure the firewall feature differently than is described in the Cisco IOS Firewall Feature Set feature module.
Configuring Windows NT

A possible problem with your Cisco 805 router in a Windows NT environment is that PCs in one network might not detect PCs in another network. This section explains how to configure the router to function in a Windows NT environment in any of the sample networks in Chapter 3, “Configuring Remote Office to Corporate Office Networks.”

Use the following table to configure the router. For information on the commands used in this table, refer to the Cisco IOS Release 12.0 documentation set.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode.</td>
<td>Router#</td>
<td>configure terminal</td>
</tr>
<tr>
<td>2</td>
<td>Forward broadcast packets destined for UDP port 137 (NetBIOS name server).</td>
<td>Router (config)#</td>
<td>ip forward-protocol udp 137</td>
</tr>
<tr>
<td>3</td>
<td>Forward broadcast packets destined for UDP port 138 (NetBIOS datagram service).</td>
<td>Router (config)#</td>
<td>ip forward-protocol udp 138</td>
</tr>
<tr>
<td>4</td>
<td>Enter configuration mode for serial interface.</td>
<td>Router (config)#</td>
<td>interface serial 0</td>
</tr>
<tr>
<td>5</td>
<td>Forward UDP broadcasts including broadcasts of IP addresses and IP configuration requests to the NT server.</td>
<td>Router (config-if)#</td>
<td>ip helper-address address</td>
</tr>
<tr>
<td>6</td>
<td>Enable interface and configuration changes just made to interface.</td>
<td>Router (config-if)#</td>
<td>no shutdown</td>
</tr>
<tr>
<td>7</td>
<td>Exit configuration mode for serial interface.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
</tbody>
</table>

The following is a sample configuration file that contains commands relevant to setting up a Windows NT environment only:

```bash
! 
ip forward-protocol udp 137
ip forward-protocol udp 138
!
serial interface 0
ip helper-address 20.1.1.1
! 
```

5-14  Cisco 805 Router Software Configuration Guide
Controlling Dial-up Line Activation

This sample configuration file configures the router to forward UDP broadcasts containing PC addresses so that PCs in network A can detect PCs in network B and vice versa (refer to Figure 5-6).

**Figure 5-6  Cisco 805 Router Forwarding UDP Broadcasts**

![Network Diagram]

However, if your network uses a dial-up line, the UDP broadcasts might activate this line too often. If keeping monthly dial-up costs low is a concern, you can control when your dial-up line is activated. For more information on this option, refer to the “Controlling Dial-up Line Activation” later in this chapter.

**Note**  An alternative to configuring the router to forward UDP broadcasts is to set up a WINS server in your network. Although WINS server setup is initially expensive, it will reduce overall traffic and eliminate the excessive dial-up line activation.

Controlling Dial-up Line Activation

This section explains how to control dial-up line activation in Network 4: Dial-up Line, PPP in Chapter 3, “Configuring Remote Office to Corporate Office Networks” and in “Network 2: Dial-up Line, PPP” in Chapter 4, “Configuring Small Office to ISP Networks.”
The following types of traffic can activate your dial-up line and increase your monthly dial-up line cost:

- UDP broadcasts associated with networks running Windows NT
- UDP broadcasts associated with networks running DHCP relay
- UDP broadcasts associated with Simple Network Time Protocol (SNTP)
- IP broadcasts, including RIP and EIGRP broadcasts
- IPX

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

**UDP Broadcasts in a Windows NT Environment**

The “Configuring Windows NT” section earlier in this chapter describes how to configure the router to forward UDP broadcasts.

To control monthly dial-up costs, you can configure an extended access list so that UDP broadcasts do not activate the dial-up line.

**Configuration**

Use the steps in this table to configure an extended access list. For information on the commands used in this table, refer to the Cisco IOS Release 12.0 documentation set.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode.</td>
<td>Router#</td>
<td>configure terminal</td>
</tr>
<tr>
<td>2</td>
<td>Enter configuration mode for serial interface.</td>
<td>Router (config)#</td>
<td>interface serial 0</td>
</tr>
<tr>
<td>3</td>
<td>Create a dialer list.</td>
<td>Router (config-if)#</td>
<td>dialer-group 1</td>
</tr>
<tr>
<td>4</td>
<td>Enable interface and configuration changes made to interface.</td>
<td>Router (config-if)#</td>
<td>no shutdown</td>
</tr>
<tr>
<td>5</td>
<td>Return to configuration mode.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
</tbody>
</table>
### UDP Broadcasts in a DHCP Relay Environment

The “Controlling Dial-up Line Activation” section earlier in this chapter described how to configure the router to forward UDP broadcasts.

To control costs, you can configure an extended access list so that UDP broadcasts do not activate the dial-up line.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Set NetBIOS name service packets to not activate dial-up line.</td>
<td>Router (config)#</td>
<td><code>access-list 100 deny udp any any eq 137</code></td>
</tr>
<tr>
<td>7</td>
<td>Set NetBIOS datagram service packets to not activate dial-up line.</td>
<td>Router (config)#</td>
<td><code>access-list 100 deny udp any any eq 138</code></td>
</tr>
<tr>
<td>8</td>
<td>Set NetBIOS session service packets to not activate dial-up line.</td>
<td>Router (config)#</td>
<td><code>access-list 100 deny tcp any any eq 139</code></td>
</tr>
<tr>
<td>9</td>
<td>Specify that extended access list 100 defines which IP packets do not activate dial-up line.</td>
<td>Router (config)#</td>
<td><code>dialer-list 100 protocol ip list 100</code></td>
</tr>
</tbody>
</table>

**Note** The extended access list developed in the task table includes some commonly anticipated restrictions. The information in this section is meant to be used as a base from which you can add or delete restrictions as they relate to your particular network. The extended access list that you create depends on your particular network.
Controlling Dial-up Line Activation

Configuration

Use the steps in this table to configure an extended access list. For information on the commands used in this table, refer to the Cisco IOS Release 12.0 documentation set.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode.</td>
<td>Router#</td>
<td>configure terminal</td>
</tr>
<tr>
<td>2</td>
<td>Enter configuration mode for serial interface.</td>
<td>Router (config)#</td>
<td>interface serial 0</td>
</tr>
<tr>
<td>3</td>
<td>Create a dialer list.</td>
<td>Router (config-if)#</td>
<td>dialer-group 1</td>
</tr>
<tr>
<td>4</td>
<td>Enable interface and configuration changes just made to interface.</td>
<td>Router (config-if)#</td>
<td>no shutdown</td>
</tr>
<tr>
<td>5</td>
<td>Return to configuration mode.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
<tr>
<td>6</td>
<td>Set location services (4-29) packets to not activate dial-up line.</td>
<td>Router (config)#</td>
<td>access-list 100 deny udp any any eq 135</td>
</tr>
<tr>
<td>7</td>
<td>Specify that extended access list 100 defines which IP packets do not activate dial-up line.</td>
<td>Router (config)#</td>
<td>dialer-list 1 protocol ip list 100</td>
</tr>
</tbody>
</table>

UDP Broadcasts in an SNTP Environment

You can configure an extended access list so that UDP broadcasts associated with SNTP do not activate the dial-up line.
Use the steps in this table to configure an extended access list. For information on the commands used in this table, refer to the Cisco IOS Release 12.0 documentation set.

## IP Traffic

You can configure an extended access list so that IP broadcasts, including RIP and EIGRP broadcasts, do not activate the dial-up line.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode.</td>
<td>Router#</td>
<td>configure terminal</td>
</tr>
<tr>
<td>2</td>
<td>Enter configuration mode for serial interface.</td>
<td>Router (config)#</td>
<td>interface serial 0</td>
</tr>
<tr>
<td>3</td>
<td>Create a dialer list.</td>
<td>Router (config-if)#</td>
<td>dialer-group 1</td>
</tr>
<tr>
<td>4</td>
<td>Enable interface and configuration changes made to interface.</td>
<td>Router (config-if)#</td>
<td>no shutdown</td>
</tr>
<tr>
<td>5</td>
<td>Return to configuration mode.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
<tr>
<td>6</td>
<td>Set SNTP packets to not activate dial-up line.</td>
<td>Router (config)#</td>
<td>access-list 100 deny udp any any eq 123</td>
</tr>
<tr>
<td>7</td>
<td>Permit other packets to and from anywhere.</td>
<td>Router (config)#</td>
<td>access-list 100 permit ip any any</td>
</tr>
<tr>
<td>8</td>
<td>Specify that extended access list 100 defines which IP packets activate dial-up line.</td>
<td>Router (config)#</td>
<td>dialer-list 1 protocol ip list 100</td>
</tr>
</tbody>
</table>
Controlling Dial-up Line Activation

Configuration

Use the steps in this table to configure an extended access list. For information on the commands used in this table, refer to the Cisco IOS Release 12.0 documentation set.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode.</td>
<td>Router#</td>
<td>configure terminal</td>
</tr>
<tr>
<td>2</td>
<td>Enter configuration mode for serial interface.</td>
<td>Router (config)#</td>
<td>interface serial 0</td>
</tr>
<tr>
<td>3</td>
<td>Create a dialer list</td>
<td>Router (config-if)#</td>
<td>dialer-group 1</td>
</tr>
<tr>
<td>4</td>
<td>Enable interface and configuration changes made to interface.</td>
<td>Router (config-if)#</td>
<td>no shutdown</td>
</tr>
<tr>
<td>5</td>
<td>Return to configuration mode.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
<tr>
<td>6</td>
<td>Set RIP packets to not activate dial-up line.</td>
<td>Router (config)#</td>
<td>access-list 100 deny udp any any eq rip</td>
</tr>
<tr>
<td>7</td>
<td>Set EIGRP packets to not activate dial-up line.</td>
<td>Router (config)#</td>
<td>access-list 100 deny eigrp any any</td>
</tr>
<tr>
<td>8</td>
<td>Permit IP packets to and from anywhere.</td>
<td>Router (config)#</td>
<td>access-list 100 permit ip any any</td>
</tr>
<tr>
<td>9</td>
<td>Specify that extended access list 100 defines which IP packets activate and do not activate dial-up line.</td>
<td>Router (config)#</td>
<td>dialer-list 1 protocol ip list 100</td>
</tr>
<tr>
<td>10</td>
<td>Enter configuration mode for serial interface.</td>
<td>Router (config)#</td>
<td>interface serial 0</td>
</tr>
<tr>
<td>11</td>
<td>Activate access list 100.</td>
<td>Router (config-if)#</td>
<td>ip access-group 100 in</td>
</tr>
<tr>
<td>12</td>
<td>Enable interface and configuration changes made to interface.</td>
<td>Router (config-if)#</td>
<td>no shutdown</td>
</tr>
<tr>
<td>13</td>
<td>Exit configuration mode for serial interface.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
</tbody>
</table>

---

Cisco 805 Router Software Configuration Guide
IPX Traffic

The following IPX protocols send updates that can cause the dial-up line to be activated excessively:

- Service Advertising Protocol (SAP)
- Routing Information Protocol (RIP)
- Serialization

To control costs, you can configure an extended access list so that SAP, RIP, and serialization packets do not activate the dial-up line.

Configuration

Use the steps in this table to configure an extended access list. For information on the commands used in this table, refer to the Cisco IOS Release 12.0 documentation set.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode.</td>
<td>Router#</td>
<td>configure terminal</td>
</tr>
<tr>
<td>2</td>
<td>Enter configuration mode for serial interface.</td>
<td>Router (config)#</td>
<td>interface serial 0</td>
</tr>
<tr>
<td>3</td>
<td>Create a dialer list.</td>
<td>Router (config-if)#</td>
<td>dialer-group 1</td>
</tr>
<tr>
<td>4</td>
<td>Enable interface and configuration changes made to interface.</td>
<td>Router (config-if)#</td>
<td>no shutdown</td>
</tr>
<tr>
<td>5</td>
<td>Return to configuration mode.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
<tr>
<td>6</td>
<td>Set SAP packets to not activate dial-up line. The value for protocol can be from 0 to 255.</td>
<td>Router (config)#</td>
<td>access-list 900 deny protocol FFFFFFFF 0 FFFFFFFF 452</td>
</tr>
<tr>
<td>7</td>
<td>Set RIP packets to not activate dial-up line. The value for protocol can be from 0 to 255.</td>
<td>Router (config)#</td>
<td>access-list 900 deny protocol FFFFFFFF 0 FFFFFFFF 453</td>
</tr>
</tbody>
</table>
Restricting Access to Your IP Network

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Set serialization packets to not activate dial-up line. The value for protocol can be from 0 to 255.</td>
<td>Router (config)#</td>
<td>access-list 900 deny protocol FFFFFFFF 0 FFFFFFFF 457</td>
</tr>
<tr>
<td>9</td>
<td>Set all IPX packets other than SAP, RIP, and serialization packets to activate dial-up line.</td>
<td>Router (config)#</td>
<td>access-list 900 permit protocol</td>
</tr>
<tr>
<td>10</td>
<td>Specify that extended access list 900 defines which IPX packets activate and do not activate dial-up line.</td>
<td>Router (config)#</td>
<td>dialer-list 1 protocol ipx list 900</td>
</tr>
</tbody>
</table>

Restricting Access to Your IP Network

This section explains how to restrict access to any of the sample networks in Chapter 4, “Configuring Small Office to ISP Networks.”

You can restrict access to your IP network by creating an extended access list. Table 5-1 provides instructions on restricting access to the sample IP network shown in Figure 5-7.

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

Figure 5-7  Restricting Access to IP Network

Network
192.168.1.0
255.255.255.0

SMTP mail server
192.168.1.2

Web server
192.168.1.3

FTP server
192.168.1.4

192.168.1.1
Cisco 805

Internet service provider

10.0.0.1

DNS server
10.0.0.3
Table 5-1  Sample IP Network-to-Internet Restrictions

<table>
<thead>
<tr>
<th>Access Permitted</th>
<th>Access Denied</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit any host on network 192.168.1.0 to access any Internet server.</td>
<td>Deny any Internet host from spoofing any host on network 192.168.1.0.  (<em>Spoofing</em> is illegally claiming to be from an address from which it is not actually sent.)</td>
</tr>
<tr>
<td>Permit any Internet domain name system (DNS) server to send TCP replies to any host on network 192.168.1.0.</td>
<td>Deny any Internet host from making a remote terminal connection (Telnet) to any host on network 192.168.1.0.</td>
</tr>
<tr>
<td>Permit any Internet DNS server to send UDP replies to any host on network 192.168.1.0.</td>
<td></td>
</tr>
<tr>
<td>Permit any Internet host to access the Simple Mail Transport Protocol (SMTP) mail server on network 192.168.1.0.</td>
<td></td>
</tr>
<tr>
<td>Permit any Internet host to access the web server on network 192.168.1.0.</td>
<td></td>
</tr>
<tr>
<td>Permit any Internet host to access the File Transport Protocol (FTP) server on network 192.168.1.0.</td>
<td></td>
</tr>
</tbody>
</table>

Configuration

Use the steps in this table to set up a sample extended access list based on the restrictions in Table 5-1. Use the information in this table as a guideline for setting up your own access list rather than necessarily configuring these settings on your router.
For information on the commands used in this table, refer to the Cisco IOS Release 12.0 documentation set. For information on TCP and UDP port assignments, refer to Appendix F, “Common Port Assignments.”

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Router Prompt</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter configuration mode.</td>
<td>Router#</td>
<td>configure terminal</td>
</tr>
<tr>
<td>2</td>
<td>Permit any host on network 192.168.1.0 to access any Internet server.</td>
<td>Router (config)#</td>
<td>access-list 100 permit tcp any 192.168.1.0 0.0.0.0 established</td>
</tr>
<tr>
<td>3</td>
<td>Deny any Internet host from spoofing any host on network 192.168.1.0.</td>
<td>Router (config)#</td>
<td>access-list 100 deny ip 192.168.1.0 0.0.0.255 any</td>
</tr>
<tr>
<td>4</td>
<td>Permit Internet DNS server to send TCP replies to any host on network 192.168.1.0.</td>
<td>Router (config)#</td>
<td>access-list 100 permit tcp host 10.0.0.3 192.168.1.0 0.0.0.255 eq 53</td>
</tr>
<tr>
<td>5</td>
<td>Permit Internet DNS server to send UDP replies to any host on network 192.168.1.0.</td>
<td>Router (config)#</td>
<td>access-list 100 permit udp host 10.0.0.3 192.168.1.0 0.0.0.255 eq 53</td>
</tr>
<tr>
<td>6</td>
<td>Permit SMTP mail server to access any Internet server.</td>
<td>Router (config)#</td>
<td>access-list 100 permit tcp any host 192.168.1.2 eq 25</td>
</tr>
<tr>
<td>7</td>
<td>Permit web server to access any Internet server.</td>
<td>Router (config)#</td>
<td>access-list 100 permit tcp any host 192.168.1.3 eq 80</td>
</tr>
<tr>
<td>8</td>
<td>Permit FTP server to access any Internet server.</td>
<td>Router (config)#</td>
<td>access-list 100 permit tcp any host 192.168.1.4 eq 21</td>
</tr>
<tr>
<td>9</td>
<td>Restrict any Internet host from making a Telnet connection to any host on network 192.168.1.0.</td>
<td>Router (config)#</td>
<td>access-list 100 deny tcp any 192.168.1.0 0.0.0.255 eq 23</td>
</tr>
<tr>
<td>10</td>
<td>Enter configuration mode for serial interface.</td>
<td>Router (config)#</td>
<td>interface serial 0</td>
</tr>
<tr>
<td>11</td>
<td>Activate access list 100.</td>
<td>Router (config-if)#</td>
<td>ip access-group 100 in</td>
</tr>
<tr>
<td>12</td>
<td>Enable interface and configuration changes made to interface.</td>
<td>Router (config-if)#</td>
<td>no shutdown</td>
</tr>
<tr>
<td>13</td>
<td>Exit configuration mode for serial interface.</td>
<td>Router (config-if)#</td>
<td>exit</td>
</tr>
</tbody>
</table>
Troubleshooting

This chapter describes what to do if you experience a problem with your router. Assuming that you do not know what the problem is, this chapter leads you through the following troubleshooting checklist:

- Verify that your router boots properly.
- Troubleshoot the physical connections:
  - Ethernet
  - Serial
- Troubleshoot Ethernet line problems.
- Troubleshoot serial line problems:
  - Clocking problems
  - Synchronous leased line problems
  - Asynchronous dial-up problems
  - Frame Relay problems
  - X.25 problems

Some of the solutions to problems that you might uncover require that you use debug commands. The chapter also contains information you need to know about these commands.

Before troubleshooting a software problem, you must connect a terminal or PC to the router light-blue Console port. (For information on making this connection, see the Cisco 805 Router Hardware Installation Guide.) With a connected terminal or PC, you can read status messages from the router and enter commands to troubleshoot a problem.
As an alternative, you can remotely access the interface (Ethernet or serial) by using Telnet. The Telnet option assumes that the interface is up and running.

Verifying that Router Boots Properly

After you power on the Cisco 805 router, the router performs a series of power-on self-tests (POSTs) to verify hardware and software operations. The following is sample output that results from a proper boot sequence:

```
TinyROM version 1.2(1)
Compiled Fri Jul 9 10:32:58 1999
Copyright (c) 1999 by cisco Systems, Inc.
All rights reserved.
POST......... OK.  8MB DRAM, 4MB Flash.
Booting up,,,
...Cisco Internetwork Operating System Software
...Press RETURN to get started!
```

If after the router boots, you cannot access the command line interface (CLI) and you get output that does not resemble the sample output, contact your Cisco reseller.
**Troubleshooting Physical Connections**

This section describes how to troubleshoot your Ethernet and serial connections.

**Ethernet Connection**

Table 6-1 describes how to troubleshoot your Ethernet connection.

<table>
<thead>
<tr>
<th>What to Look for</th>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the LINK LED on the router back panel blinking or off? If blinking or off, then go on to the Problems column. If on, then go on the “Serial Connection” section.</td>
<td>No connection to Ethernet device, which can be caused by one of the following:</td>
<td>Perform the following tasks in the following order:</td>
</tr>
<tr>
<td></td>
<td>• A cable-related problem:</td>
<td><strong>Step 1</strong>  To make sure you have cabled the device correctly, refer to the installation chapter in the <em>Cisco 805 Router Hardware Installation Guide</em>.</td>
</tr>
<tr>
<td></td>
<td>— Improperly connected cable.</td>
<td><strong>Step 2</strong>  Make sure the connectors at both ends of the cable are securely seated.</td>
</tr>
<tr>
<td></td>
<td>— Damaged cable.</td>
<td><strong>Step 3</strong>  Make sure the cable is not physically damaged. If it is, order another cable from Cisco or replace it with a similar cable.</td>
</tr>
<tr>
<td></td>
<td>• Improperly set router HUB/NO HUB button or hub equivalent of HUB/NO HUB button.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To make sure you have set button(s) correctly, refer to the installation chapter in the <em>Cisco 805 Router Hardware Installation Guide</em>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Improperly functioning network interface card (NIC) on server, PC, or workstation.</td>
<td>• Run the NIC diagnostic supplied by the vendor to make sure it is functioning properly. If it is not, replace it.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the problem continues after these checks, call your Cisco reseller.</td>
</tr>
</tbody>
</table>
Serial Connection

Table 6-2 describes how to troubleshoot your serial connection.

<table>
<thead>
<tr>
<th>What to Look for</th>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the CD LED on the router front panel off for a long time? If off, then go on to the Problems column. If on, then go on the “Troubleshooting Ethernet Line Problems” section.</td>
<td>No connection to serial device, which can be caused by one of the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Wrong cable.</td>
<td>To make sure you are using the correct cable, refer to Appendix A, “Selecting a Serial Cable” in the Cisco 805 Router Hardware Installation Guide.</td>
</tr>
<tr>
<td></td>
<td>• Improperly connected cable.</td>
<td>• To make sure that you have cabled properly, refer to the installation chapter in the Cisco 805 Router Hardware Installation Guide.</td>
</tr>
<tr>
<td></td>
<td>• Improperly functioning modem or channel service unit/data service unit (CSU/DSU).</td>
<td>• Make sure the connectors at both ends of the cable are securely seated.</td>
</tr>
<tr>
<td></td>
<td>• CSU/DSU configuration has been lost or changed.</td>
<td>Refer to the documentation that accompanies your modem or CSU/DSU.</td>
</tr>
<tr>
<td></td>
<td>• Router improperly configured as a data terminal equipment (DTE) or data communications equipment (DCE).</td>
<td>Check CSU/DSU configuration. If necessary, reconfigure CSU/DSU so that its settings match original provisioning parameters provided by your WAN service provider.</td>
</tr>
</tbody>
</table>
Troubleshooting Ethernet Line Problems

Use the following steps to troubleshoot problems with your Ethernet line:

**Step 1** Enter the `show interfaces ethernet 0` privileged EXEC command.

**Step 2** Check the output for the following:
- Make sure that the interface is up.
- Make sure that the interface has an IP address (Internet address) assigned.
- Make sure that the IP address and subnet mask assigned to the interface match your IP addressing scheme.

**Step 3** Refer to Table 6-3 if one of the following applies:
- The Ethernet interface is administratively down.
- The Ethernet interface does not have an IP address.
- The IP address and subnet mask assigned to the Ethernet interface do not match your IP addressing scheme.

<table>
<thead>
<tr>
<th>Table 6-3</th>
<th>Problems with Serial Connection (continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What to Look for</strong></td>
<td><strong>Problems</strong></td>
</tr>
<tr>
<td>Serial interface has been shut down.</td>
<td></td>
</tr>
<tr>
<td>Problem with serial line or WAN service.</td>
<td></td>
</tr>
</tbody>
</table>

**Troubleshooting Ethernet Line Problems**

Use the following steps to troubleshoot problems with your Ethernet line:

**Step 1** Enter the `show interfaces ethernet 0` privileged EXEC command.

**Step 2** Check the output for the following:
- Make sure that the interface is up.
- Make sure that the interface has an IP address (Internet address) assigned.
- Make sure that the IP address and subnet mask assigned to the interface match your IP addressing scheme.

**Step 3** Refer to Table 6-3 if one of the following applies:
- The Ethernet interface is administratively down.
- The Ethernet interface does not have an IP address.
- The IP address and subnet mask assigned to the Ethernet interface do not match your IP addressing scheme.

<table>
<thead>
<tr>
<th>Table 6-3</th>
<th>Ethernet Line Problems</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Problems</strong></td>
<td><strong>Solutions</strong></td>
</tr>
<tr>
<td>Interface is administratively down.</td>
<td>Enter the <code>no shutdown</code> command in Ethernet interface configuration mode to bring the Ethernet interface up.</td>
</tr>
<tr>
<td>Interface does not have an IP address.</td>
<td>Assign an IP address and subnet mask to the interface by entering the <code>ip address ip-address mask</code> command in Ethernet interface configuration mode.</td>
</tr>
</tbody>
</table>
Troubleshooting Serial Line Problems

Table 6-3  Ethernet Line Problems (continued)

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address and subnet mask assigned to interface do not match your IP addressing scheme.</td>
<td>Assign the correct IP address and subnet mask to the interface by entering the <code>ip address ip-address mask</code> command in Ethernet interface configuration mode.</td>
</tr>
</tbody>
</table>

Troubleshooting Serial Line Problems

This section describes how to troubleshoot problems in the following areas:

- Synchronous CSU/DSU clocking
- Synchronous leased lines
- Asynchronous dial-up lines
- Frame Relay
- X.25

Synchronous CSU/DSU Clocking Problems

Clocking conflicts in serial connections can lead to either chronic loss of connection service or to degraded performance. This section describes how to detect and solve clocking problems with synchronous CSU/DSUs.

Detecting Problems

Use the following steps to detect clocking conflicts on your serial interface:

**Step 1** Enter the `show interfaces serial 0` privileged EXEC command on the routers at both ends of the link.

**Step 2** Examine the output for cyclic redundancy check (CRC) or framing errors and aborts.

If the number of CRC or framing errors exceeds an approximate range of 0.5 to 2.0 percent of traffic on the serial interface, clocking problems are likely to exist somewhere in the WAN.
Step 3  Isolate the source of the clocking conflicts by performing a series of ping tests and loopback tests (both local and remote).

For information on how to perform ping and loopback tests, refer to the “Performing Ping Tests” and “Performing Loopback Tests” sections later in this chapter.

Step 4  Reenter the `show interfaces serial 0` privileged EXEC command on the routers at both ends of the link. Determine if CRC and framing errors are increasing and if so, where they are accumulating.

If input errors are accumulating on both ends of the connection, clocking of the CSU is the likely problem. If input errors are accumulating on one end of the connection, clocking of the DSU or cabling are the likely problems. If aborts are occurring on one end of the connection, the other end could be sending bad information or there could be a problem with the serial line. For information on how to solve these problems, refer to Table 6-4.

### Table 6-4  Synchronous CSU/DSU Clocking Problems

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorrect CSU configuration.</td>
<td>Perform the following tasks in the following order:</td>
</tr>
<tr>
<td></td>
<td><strong>Step 1</strong> Determine if the CSUs at both ends of the serial line agree on the clock source (local or line).</td>
</tr>
<tr>
<td></td>
<td><strong>Step 2</strong> If the CSUs do not agree, configure them so that they do (usually the line is the source).</td>
</tr>
<tr>
<td></td>
<td><strong>Step 3</strong> Check the line build out (LBO) setting on the CSU to ensure that the impedance matches that of the physical line. For information on configuring your CSU, refer to your CSU documentation.</td>
</tr>
</tbody>
</table>
Troubleshooting Serial Line Problems

Performing Ping Tests

Use the following steps to perform ping tests:

Step 1 Put the CSU or DSU into local loopback mode.

Step 2 Use the ping privileged EXEC command to send different data patterns and packet sizes.

Figure 6-1 and Figure 6-2 illustrate two useful ping tests, an all-zeros 1500-byte ping and an all-ones 1500-byte ping, respectively.

Table 6-4 Synchronous CSU/DSU Clocking Problems (continued)

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorrect DSU configuration.</td>
<td>Perform the following steps in the following order:</td>
</tr>
<tr>
<td></td>
<td><strong>Step 1</strong> Determine if the DSUs at both ends of the serial line have serial clock transmit external (SCTE) mode enabled.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 2</strong> If SCTE is not enabled on both ends of the connection, enable it.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 3</strong> For any interface that is connected to a line of 128 kbps or faster, SCTE <em>must</em> be enabled.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 4</strong> Make sure that ones density is maintained, which requires that the DSU use the same framing and coding schemes (for example, Extended Superframe Format [ESF] and Binary 8-Zero Substitution [B8ZS]) used by the leased line or other carrier service.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 5</strong> Check with your leased line provider for information on their framing and coding schemes.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 6</strong> If your carrier service uses Alternate Mark Inversion (AMI) coding, either invert the transmit clock on both sides of the link or run the DSU in bit-stuff mode. For information on configuring your DSU, refer to your DSU documentation.</td>
</tr>
</tbody>
</table>

Cable to router out of specification. For information on the appropriate cable needed to connect a serial device to a Cisco 805 router, refer to Appendix A, “Selecting a Serial Cable” in the *Cisco 805 Router Hardware Installation Guide*. For information on the appropriate cable needed to connect a serial device to the other router, refer to your router documentation.

6-8 Cisco 805 Router Software Configuration Guide
Synchronous CSU/DSU Clocking Problems

Figure 6-1 All-Zeros 1500-Byte Ping Test

```
yowzers# ping
Protocol [ip]:
Target IP address: 192.169.51.22
Repeat count [5]: 100
Datagram size [100]: 1500
Timeout in seconds [2]:
Extended commands [n]: y
Source address: 192.169.51.14
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]: 0x0000
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 1500-byte ICMP Echos to 192.169.51.22, timeout is 2 seconds:
Packet has data pattern 0x0000
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 4/6/8 ms
yowzers#
```
Performing Loopback Tests

These loopback tests do not apply to Frame Relay or X.25 networks. Figure 6-3 shows the basic topology of the CSU/DSU local and remote loopback tests.
Local Loopback Tests

Use the following steps to perform local loopback tests:

**Step 1** Place the CSU/DSU in local loop mode (refer to your CSU/DSU documentation).

In local loop mode, the use of the line clock (from the T1 service) is terminated, and the DSU is forced to use the local clock.

**Step 2** Enter the `show interfaces serial 0` privileged EXEC command to determine if the line status changes from “line protocol is down” to “line protocol is up (looped),” or if it remains down.

If the line protocol comes up when the CSU or DSU is in local loopback mode, a problem could be occurring on the remote end of the serial connection. If the status line does not change state, there is a possible problem in the router, connecting cable, or CSU/DSU.

If the problem appears to be local, enter the `debug serial interface` privileged EXEC command and go on to the next step.

**Step 3** Take the CSU/DSU out of local loop mode.

When the line protocol is down, the `debug serial interface` command output will indicate that keepalive counters are not incrementing.

**Step 4** Place the CSU/DSU in local loop mode again.

This action should cause the keepalive packets to begin to increment. Specifically, the values for *mineseen* and *yourseen* keepalives will increment every 10 seconds. This information will appear in the `debug serial interface` output.

If the keepalives do not increment, there may be a timing problem on the interface card or on the network.

**Step 5** Check the local router and CSU/DSU hardware, and any attached cables.

Make certain the cables are within the recommended lengths (no more than 50 feet [15.24 meters], or 25 feet [7.62 meters] for a T1 link). Make certain the cables are attached to the proper ports. Swap faulty equipment as necessary.
Troubleshooting Serial Line Problems

Remote Loopback Tests
Use the following steps to perform remote loopback tests:

**Step 1**  
Put the remote CSU or DSU into remote loopback mode (refer to your CSU/DSU documentation).

**Step 2**  
Enter the `show interfaces serial 0` privileged EXEC command to determine if the line protocol remains up with the status line indicating “Serial x is up, line protocol is up (looped),” or if it goes down with the status line indicating “line protocol is down.”

If the line protocol remains up (looped), the problem is probably at the remote end of the serial connection (between the remote CSU/DSU and the remote router). Perform both local and remote tests at the remote end to isolate the problem source.

If the line status changes to “line protocol is down” when remote loopback mode is activated, make certain that ones density is being properly maintained. The CSU/DSU must be configured to use the same framing and coding schemes used by the leased-line or other carrier service (for example, ESF and B8ZS).

Synchronous Leased Line Problems
Use the following steps to troubleshoot problems with your synchronous leased line:

**Step 1**  
From privileged EXEC command mode, enter the `show interfaces serial 0` command.

If you see the line `Serial0 is up, line protocol is up`, the serial line is functioning properly. You do not need to take further action.

**Step 2**  
If you see one of the following messages, refer to Table 6-5:

- Serial 0 is down, line protocol is down.
- Serial 0 is up, line protocol is down.
- Serial 0 is up, line protocol is up (looped).
- Serial 0 is administratively down, line protocol is up.
## Table 6-5  Leased Line Problems

<table>
<thead>
<tr>
<th>Line State</th>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
</table>
| Serial 0 is down, line protocol is down. | The router is not sensing a carrier detect (CD) signal due to one of the following reasons:  
• Faulty or incorrect cabling of the router.  
• Local router hardware failure.  
• Local CSU/DSU hardware failure.  
• WAN service provider problem, such as the line is down or not connected to the CSU/DSU. | Following are some steps you can take to isolate the problem:  
• Refer to the *Cisco 805 Router Hardware Installation Guide* to confirm that you are using the correct serial cable to connect the CSU/DSU and that you connected the CSU/DSU correctly.  
• Connect the leased line to another port, if possible. If the connection comes up, there is a hardware failure. Contact your Cisco reseller.  
• Check the LEDs on the CSU/DSU for CD activity.  
• Contact your WAN service provider. |
Troubleshooting Serial Line Problems

Table 6-5  Leased Line Problems (continued)

<table>
<thead>
<tr>
<th>Line State</th>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial 0 is up, line protocol is down.</td>
<td>Possible causes for this line state are:</td>
<td>Following are some steps you can take to isolate the problem:</td>
</tr>
<tr>
<td></td>
<td>• Router hardware failure.</td>
<td>• Refer to the <em>Cisco 805 Router Hardware Installation Guide</em> to confirm that you are using the correct serial cable to connect the CSU/DSU and that you connected the CSU/DSU correctly.</td>
</tr>
<tr>
<td></td>
<td>• Local or remote CSU/DSU hardware failure.</td>
<td>• Connect the leased line to another port, if possible. If the connection comes up, there is a hardware failure. Contact your Cisco reseller.</td>
</tr>
<tr>
<td></td>
<td>• Local or remote router misconfigured.</td>
<td>• Check the LEDs on the CSU/DSU for CD activity.</td>
</tr>
<tr>
<td></td>
<td>• The serial clock transmit external is not set on the CSU/DSU.</td>
<td>• Perform CSU/DSU loopback tests. During local loopback, enter the <code>show interfaces serial 0</code> command. If the line protocol is shown as up, there might be a problem with the WAN service provider, or the remote router is down.</td>
</tr>
<tr>
<td></td>
<td>• The remote router is not sending keepalive packets.</td>
<td>• Contact your WAN service provider.</td>
</tr>
<tr>
<td></td>
<td>• Problem with the leased line.</td>
<td></td>
</tr>
</tbody>
</table>

Table 6-5  Leased Line Problems (continued)
## Troubleshooting

### Synchronous Leased Line Problems

The possible cause is that a loop exists in the circuit. The sequence number in the keepalive packet changes to a random number when a loop is first detected. If the same random number is returned over the line, a loop exists.

Following are some steps you can take to isolate the problem:

- Use the `write terminal` privileged EXEC command to display any instances of the loopback command. If the router has been configured with the loopback command, enter the `no loopback` command to remove the loop.
- Check to see if the CSU/DSU is configured in manual loopback mode. If it is, disable manual loopback.
- Reset the CSU/DSU.
- If you are unable to isolate the problem, contact your WAN service provider for help with troubleshooting.

### Table 6-5  Leased Line Problems (continued)

<table>
<thead>
<tr>
<th>Line State</th>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial 0 is up, line protocol is up (looped).</td>
<td>The possible cause is that a loop exists in the circuit. The sequence</td>
<td>Following are some steps you can take to isolate the problem:</td>
</tr>
<tr>
<td></td>
<td>number in the keepalive packet changes to a random number when a loop is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>is first detected. If the same random number is returned over the line,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a loop exists.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Use the <code>write terminal</code> privileged EXEC command to display any</td>
</tr>
<tr>
<td></td>
<td></td>
<td>instances of the loopback command. If the router has been configured</td>
</tr>
<tr>
<td></td>
<td></td>
<td>with the loopback command, enter the <code>no loopback</code> command to remove the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>loop.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check to see if the CSU/DSU is configured in manual loopback mode. If</td>
</tr>
<tr>
<td></td>
<td></td>
<td>it is, disable manual loopback.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Reset the CSU/DSU.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If you are unable to isolate the problem, contact your WAN service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>provider for help with troubleshooting.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Serial 0 is administratively down, line</td>
<td>The possible causes for this state are:</td>
<td></td>
</tr>
<tr>
<td>protocol is up.</td>
<td>• The serial interface has been disabled with the <code>shutdown</code> command.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Different interfaces on the router are using the same IP address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Following are some steps you can take to isolate the problem:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Use the <code>show configuration</code> privileged EXEC command to display the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>serial port configuration. If &quot;shutdown&quot; is displayed after</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;interface Serial0,&quot; use the <code>no shutdown</code> command in serial interface</td>
</tr>
<tr>
<td></td>
<td></td>
<td>configuration mode to enable the interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Use the <code>show interface</code> privileged EXEC command to display the IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>addresses for all router interfaces. Take the appropriate action to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>assign a unique IP address to each router interface. (If you set up your</td>
</tr>
<tr>
<td></td>
<td></td>
<td>network per the sample networks in the this guide, refer to that</td>
</tr>
<tr>
<td></td>
<td></td>
<td>particular sample network for information on how to assign a unique</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IP address to the router interfaces.</td>
</tr>
</tbody>
</table>
Asynchronous Dial-up Problems

This section describes how to use the `show line 1` command to troubleshoot problems with the connection between your modem and router. It also describes the following symptoms, problems, and solutions:

- No Connectivity between Modem and Router
- Modem Does Not Dial
- Modem Does Not Answer
- Modem Hangs Up Shortly after Connecting
- Dial-up Client Receives No EXEC Prompt
- Dial-up Session Sees Garbage
- Dial-up Session Ends Up in Existing Session
- Modem Cannot Send or Receive Data
- Modem Cannot Send or Receive IP Data
- Modem Cannot Send or Receive IPX Data
- Modem Does Not Disconnect Properly
- Link Goes Deactivates Soon
- Link Does Not Deactivate or Stays Activated Too Long
- Poor Performance

Troubleshooting Problems with Modem and Router Connection

Use the following steps to troubleshoot problems with the connection between your modem and router:

**Step 1**  From privileged EXEC command mode, enter the `show line 1` command.

Check the Modem state field in the output. If the modem state is Idle and CTS noDSR DTR RTS, the connection between your modem and router is functioning properly.
Step 2  If you see one of the following modem states, refer to Table 6-6:

- Ready –
- Ready not CTS noDSR DTR RTS
- Ready CTS DSR DTR RTS
- Ready CTS* DSR* DTR RTS

Table 6-6  Problems with Modem and Router Connection

<table>
<thead>
<tr>
<th>Modem State</th>
<th>Problems</th>
</tr>
</thead>
</table>
| Ready –     | • Modem control is not configured on the router. Enter the `modem inout` command in serial interface configuration mode.  
• A session exists on the line. Enter the `show users` privileged EXEC command and the `clear line 0` privileged EXEC command to stop the session if desired.  
• Data set ready (DSR) is high. There are two possible reasons for this:  
  — Cabling problems—If your modem connector uses DB-25 pin 6 and has no pin 8, you must move the pin from 6 to 8 or get the appropriate connector.  
  — Modem configured for data carrier detect (DCD) always high—The modem should be reconfigured to have DCD high only on carrier detect (CD), which is usually done with the `&C1` modem command. Check your modem documentation for the exact syntax for your modem.  
  If your software does not support modem control, you must configure the router line to which the modem is connected with the `no exec` command in asynchronous line configuration mode. Clear the line with the `clear line` privileged EXEC command, initiate a reverse Telnet session with the modem, and reconfigure the modem so that DCD is high only on CD. End the Telnet session by entering `disconnect` and reconfigure the router line with the `exec` command in asynchronous line configuration mode. |
Troubleshooting Serial Line Problems

Table 6-6 Problems with Modem and Router Connection (continued)

<table>
<thead>
<tr>
<th>Modem State</th>
<th>Problems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ready noCTS noDSR DTR RTS</td>
<td>• The modem is turned off.</td>
</tr>
<tr>
<td></td>
<td>• The modem is not properly connected to the router. Refer to the Cisco 805 Router Hardware Installation Guide for information on how to select the serial cable and how to connect the modem.</td>
</tr>
<tr>
<td></td>
<td>• The modem is not configured for hardware flow control. Disable hardware flow control on the router by entering the no flowcontrol hardware command in asynchronous line configuration mode. Enable hardware flow control on the modem via a reverse Telnet session. (Consult your modem documentation.) Reenable hardware flow control on the router by entering the flowcontrol hardware command in asynchronous line configuration mode.</td>
</tr>
<tr>
<td>Ready CTS DSR DTR RTS</td>
<td>• Incorrect cabling. Refer to the Cisco 805 Router Hardware Installation Guide for information on how to select the serial cable.</td>
</tr>
<tr>
<td></td>
<td>• The modem is configured for DCD always high. Reconfigure the modem so that DCD is only high on CD, which is usually done with the &amp;C1 modem command. Check your modem documentation for the exact syntax for your modem. Configure the router line to which the modem is connected by entering the no exec command in asynchronous line configuration mode. Clear the line with the clear line privileged EXEC command, initiate a reverse Telnet session with the modem, and reconfigure the modem so that DCD is high only on CD. End the Telnet session by entering disconnect. Reconfigure the router line with the exec command in asynchronous line configuration mode.</td>
</tr>
<tr>
<td>Ready CTS* DSR* DTR RTS</td>
<td>If this string appears in the Modem state field, modem control is probably not enabled on the router. Enter the modem inout command in asynchronous line configuration mode to enable modem control on the line.</td>
</tr>
</tbody>
</table>

1 An asterisk (*) next to a signal indicates one of two things: the signal has changed within the last few seconds, or the signal is not being used by the modem control method selected.

No Connectivity between Modem and Router

**Symptom:** The connection between a modem and a Cisco router does not work. Attempts to initiate a reverse Telnet session to the modem have no result, or the user receives a “Connection Refused by Foreign Host” message.
Asynchronous Dial-up Problems

Note  More specific symptoms for dial-up connection problems are covered later in this section.

Table 6-7 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 6-7  No Connectivity between Modem and Router

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorrect cabling</td>
<td>Check the cabling between the modem and the router. Refer to the Cisco 805 Router Hardware Installation Guide for information on how to select the serial cable and how to connect the modem.</td>
</tr>
<tr>
<td>Hardware problem</td>
<td>• Check the cabling between the modem and the router. Refer to the Cisco 805 Router Hardware Installation Guide for information on how to select the serial cable and how to connect the modem.</td>
</tr>
<tr>
<td></td>
<td>• Check all hardware for damage, including cabling (broken wires), adapters (loose pins), ports, and modem.</td>
</tr>
<tr>
<td>Modem control is not enabled on the router</td>
<td>• Use the show line 1 privileged EXEC command on the router. The output should show inout or RIisCD in the Modem column, which indicates that modem control is enabled on the line of the router.</td>
</tr>
<tr>
<td></td>
<td>• If necessary, configure modem control by using the modem inout command in asynchronous line configuration mode.</td>
</tr>
</tbody>
</table>

Modem Does Not Dial

Symptom: Dial-up sessions cannot be established because the modem does not dial properly.

Table 6-8 outlines the problems that might cause this symptom and describes solutions to those problems.
Troubleshooting Serial Line Problems

Table 6-8 Modem Does Not Dial

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorrect cabling</td>
<td>Check the cabling between the modem and the router. Refer to the Cisco 805 Router Hardware Installation Guide for information on how to select the serial cable and how to connect the modem.</td>
</tr>
<tr>
<td>Modem hardware problem</td>
<td>Check the modem's physical connection. Make sure the modem is on and is connected securely to the correct port. Make sure the transmit and receive indicator lights flash when the chat script is running.</td>
</tr>
</tbody>
</table>
| No interesting packets defined| • Use the show running-config privileged EXEC command to view the router configuration. Check the dialer-list command entries to see which access lists, if any, are being used to define interesting traffic.  
  • Make sure that the access lists referenced by the dialer-list commands specify all traffic that should bring the link up (interesting traffic).  
  • If necessary, modify the access list commands so that they define the proper traffic as interesting. |
| Missing chat script           | • Use the debug chat privileged EXEC command to check if there is a chat script running.  
  • If there is no chat script running, use the start-chat privileged EXEC command or another appropriate command to start the chat script on the line.  
  For detailed information about creating and configuring chat scripts, refer to the Dial Solutions Configuration Guide. |
| Bad chat script               | • Establish a reverse Telnet session to the modem, and step through each step of the chat script.  
  • Verify that the command response to each chat script step is correct.  
  • Fix any inconsistencies you find in the chat script.  
  For detailed information about creating and configuring chat scripts, refer to the Dial Solutions Configuration Guide. |
Modem Does Not Answer

**Symptom:** When attempting to open a dial-up connection to a modem, the modem does not answer the call.

Table 6-9 outlines the problems that might cause this symptom and describes solutions to those problems.

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorrect cabling</td>
<td>Check the cabling between the modem and the router. Refer to the Cisco 805 Router Hardware Installation Guide for information on how to select the serial cable and how to connect the modem.</td>
</tr>
</tbody>
</table>
| Modem control not enabled on router | • Observe the remote modem to see if it is receiving a data terminal ready (DTR) signal from the router. Most modems have a DTR indicator light. Check the modem documentation to interpret the indicator lights.  
  • If the DTR indicator light is on, the modem is seeing a DTR signal from the router. You can also enter the `show line 1` privileged EXEC command to check for DTR. If the Modem state shows the string `noDTR`, then the router is configured to hold DTR low and the modem is not seeing a DTR signal.  
  • Configure modem control by entering either the `modem inout` or the `modem ri-is-cd` command in the asynchronous line configuration mode. |
| Remote modem not set to auto-answer | • Check the remote modem to see if it is set to auto-answer. Usually, an AA indicator light will be on when auto-answer is set.  
  • Set the remote modem to auto-answer if it is not already set. To find out how to verify and change the modem's settings, refer to your modem documentation. |
| Wrong telephone line attached to remote modem | • Make sure you are using the correct telephone line. Replace the remote modem with a telephone and call again. If the phone rings, you are using the correct telephone line.  
  • Contact the telephone company to make sure that the line is good. |
| Remote modem not attached to a router | • Make sure the remote modem is attached to a router or other device that is asserting DTR.  
  • Most modems have an LED indicator for DTR. Check to make sure this indicator comes on. |
Troubleshooting Serial Line Problems

Modem Hangs Up Shortly after Connecting

**Symptom:** A dial-up connection is successful but the modem hangs up after 30 to 90 seconds.

Table 6-10 outlines the problems that might cause this symptom and describes solutions to those problems.

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
</table>
| Modem speed setting is not locked | • Enter the **show line 1** privileged EXEC command on the router. The output for the serial port should indicate the currently configured transmit (Tx) and receive (Rx) speeds.  
• If the line is not configured to the correct speed, use the **speed** command in asynchronous line configuration mode to set the speed on the router line. Set the value to the highest speed in common between the modem and the router port. If for some reason you cannot use flow control, limit the line speed to 9600 bps. Faster speeds are likely to result in lost data.  
• Use the **show line 1** command again, and confirm that the line speed is set to the desired value.  
• When you are certain that the router line is configured for the desired speed, initiate a reverse Telnet session to the modem on that line.  
• Use a modem command string that includes the lock DTE speed command for your modem. See your modem documentation for exact configuration command syntax. The lock DTE speed command, which might also be referred to as **port rate adjust or buffered mode**, is often related to the way in which the modem handles error correction. This command varies widely between modems.  
Locking the modem speed ensures that the modem always communicates with the Cisco router at the speed configured on the Cisco serial port. If this command is not used, the modem will revert to the speed of the data link (the telephone line) instead of communicating at the speed configured on the router. |
Asynchronous Dial-up Problems

Table 6-10  Modem Hang Up Shortly after Connecting (continued)

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
</table>
| Modem control is not enabled    | - Use the `show line 1` privileged EXEC command on the router. The output for the port should show `inout` or `RIisCD` in the Modem column, which indicates that modem control is enabled on the line of the router.  
  - If necessary, configure modem control by using the `modem inout` command in asynchronous line configuration mode. |
| PPP authentication fails        | - Use the `debug ppp chap` privileged EXEC command to see if PPP authentication was successful. Check the output for the phrase `Passed authentication with remote`. If you see this output, authentication was successful.  
  - If PPP authentication was not successful, verify the username and password configured on the router. The username and password you enter must be identical to those configured on the router. Usernames and passwords are case-sensitive. |
| Local router not waiting long   | - Enter the `show dialer` privileged EXEC command to see the configured dialer timeout. A timeout value of less than 120 seconds will not be long enough.  
  - Configure the local router to wait longer for the connection by entering the `dialer wait-for-carrier-time` command in the serial interface configuration mode. Make sure you specify at least a 120-second timeout. |
| Chat script problem             | - Enter the `debug chat` privileged EXEC command. If you see the output “Success” at the end of the chat script, the chat script completed successfully.  
  - Make the timeout in the chat script longer at the point where it fails.  
  - If the problem persists, verify that the command response to each chat script step is correct. Open a reverse Telnet session to the modem and step through the chat script.  
  - Fix any inconsistencies you find in the chat script.  
  For detailed information about creating and configuring chat scripts, refer to the Dial Solutions Configuration Guide. |

Dial-up Client Receives No EXEC Prompt

**Symptom:** A remote dial-up client opens a session and appears to be connected, but the user does not receive an EXEC prompt (for example, a `Username>` or `Router>` prompt).

Table 6-11 outlines the problems that might cause this symptom and describes solutions to those problems.
Troubleshooting Serial Line Problems

Table 6-11   Dial-up Client Receives No EXEC Prompt

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autoselect is enabled on the line</td>
<td>Try to access privileged EXEC mode by entering a carriage return.</td>
</tr>
<tr>
<td>Line is configured with the no exec command</td>
<td>- Use the <strong>show line 1</strong> privileged EXEC command to view the status of the appropriate line. Check the Capabilities field to see if it says <strong>EXEC suppressed</strong>. If this is the case, the <strong>no exec</strong> line configuration command is enabled.</td>
</tr>
<tr>
<td></td>
<td>- Configure the <strong>exec</strong> command in asynchronous line configuration mode to allow EXEC sessions to be initiated.</td>
</tr>
<tr>
<td>Flow control is not enabled, is enabled only on one device (either DTE or DCE), or is misconfigured</td>
<td>- Enter the <strong>show line 0</strong> privileged EXEC command, and look for the following in the Capabilities field:</td>
</tr>
<tr>
<td></td>
<td>Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out...</td>
</tr>
<tr>
<td></td>
<td>If there is no mention of hardware flow control in this field, hardware flow control is not enabled on the line.</td>
</tr>
<tr>
<td></td>
<td>- Configure hardware flow control on the line using the <strong>flowcontrol hardware</strong> command in asynchronous line configuration mode. If for some reason you cannot use flow control, limit the line speed to 9600 bps. Faster speeds are likely to result in lost data.</td>
</tr>
<tr>
<td></td>
<td>- After enabling hardware flow control on the router line, initiate a reverse Telnet session to the modem via that line.</td>
</tr>
<tr>
<td></td>
<td>- Use a modem command string that includes the RTS/CTS Flow command for your modem. This command ensures that the modem is using the same method of flow control (that is, hardware flow control) as the Cisco router. See your modem documentation for exact configuration command syntax.</td>
</tr>
</tbody>
</table>
Asynchronous Dial-up Problems

Table 6-11  Dial-up Client Receives No EXEC Prompt (continued)

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modem speed setting is not locked</td>
<td>• Enter the show line 1 privileged EXEC command on the router. The output for the serial port should indicate the currently configured transmit (Tx) and receive (Rx) speeds.</td>
</tr>
<tr>
<td></td>
<td>• If the line is not configured to the correct speed, use the speed command in asynchronous line configuration mode to set the speed on the router line. Set the value to the highest speed in common between the modem and the router port. If for some reason you cannot use flow control, limit the line speed to 9600 bps. Faster speeds are likely to result in lost data.</td>
</tr>
<tr>
<td></td>
<td>• Use the show line 1 command again, and confirm that the line speed is set to the desired value.</td>
</tr>
<tr>
<td></td>
<td>• When you are certain that the router line is configured for the desired speed, initiate a reverse Telnet session to the modem on that line.</td>
</tr>
<tr>
<td></td>
<td>• Use a modem command string that includes the lock DTE speed command for your modem. See your modem documentation for exact configuration command syntax.</td>
</tr>
<tr>
<td></td>
<td>The lock DTE speed command, which might also be referred to as port rate adjust or buffered mode, is often related to the way in which the modem handles error correction. This command varies widely between modems.</td>
</tr>
<tr>
<td></td>
<td>Locking the modem speed ensures that the modem always communicates with the Cisco router at the speed configured on the Cisco serial port. If this command is not used, the modem will revert to the speed of the data link (the telephone line) instead of communicating at the speed configured on the router.</td>
</tr>
</tbody>
</table>

Dial-up Session Sees Garbage

**Symptom:** Attempts to establish remote dial-up sessions over a modem to a Cisco router return garbage and ultimately result in no connection to the remote site. Users might see a Connection Closed by Foreign Host message.

Table 6-12 outlines the problems that might cause this symptom and describes solutions to those problems.
Troubleshooting Serial Line Problems

Table 6-12  Dial-up Session Sees Garbage

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
</table>
| Modem speed setting is not locked      | • Enter the **show line 1** privileged EXEC command on the router. The output for the serial port should indicate the currently configured transmit (Tx) and receive (Rx) speeds.  
• If the line is not configured to the correct speed, use the **speed** command in asynchronous line configuration mode to set the speed on the router line. Set the value to the highest speed in common between the modem and the router port. If for some reason you cannot use flow control, limit the line speed to 9600 bps. Faster speeds are likely to result in lost data.  
• Use the **show line 1** command again, and confirm that the line speed is set to the desired value.  
• When you are certain that the router line is configured for the desired speed, initiate a reverse Telnet session to the modem on that line.  
• Use a modem command string that includes the lock DTE speed command for your modem. See your modem documentation for exact configuration command syntax.  

The lock DTE speed command, which might also be referred to as *port rate adjust* or *buffered mode*, is often related to the way in which the modem handles error correction. This command varies widely between modems.  

Locking the modem speed ensures that the modem always communicates with the Cisco router at the speed configured on the Cisco serial port. If this command is not used, the modem will revert to the speed of the data link (the telephone line) instead of communicating at the speed configured on the router. |

Dial-up Session Ends Up in Existing Session

**Symptom:** Remote dial-up session ends up in an already existing session initiated by another user. That is, instead of getting a login prompt, a dial-up user sees a session established by another user (which might be a UNIX command prompt, a text editor session, and so forth).

Table 6-13 outlines the problems that might cause this symptom and describes solutions to those problems.
Asynchronous Dial-up Problems

Table 6-13  Dial-up Session Ends Up in Existing Session

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorrect cabling</td>
<td>Check the cabling between the modem and the router. Refer to the <em>Cisco 805 Router Hardware Installation Guide</em> for information on how to select the serial cable and how to connect the modem.</td>
</tr>
</tbody>
</table>
| Modem control is not enabled on the router | • Enter the **show line 1** privileged EXEC command on the router. The output for the serial port should show **inout** or **RIisCD** in the Modem column, which indicates that modem control is enabled on the router line.  
  • Configure modem control by entering either the **modem inout** or the **modem ri-is-cd** command in the asynchronous line configuration mode. |
| Modem configured for DCD is always high | • The modem should be reconfigured to have DCD high only on CD, which is usually configured with the **&C1** modem command string. Check your modem documentation for the exact syntax for your modem.  
  • You might have to configure the router line to which the modem is connected with the **no exec** command in asynchronous line configuration mode. Clear the line with the **clear line** privileged EXEC command, initiate a reverse Telnet session with the modem, and reconfigure the modem so that DCD is high only on CD.  
  • End the Telnet session by entering **disconnect** and reconfigure the router line with the **exec** line configuration command. |

Modem Cannot Send or Receive Data

**Symptom:** After a dial-up connection is established, a modem cannot send or receive data of any kind.

Table 6-14 outlines the problems that might cause this symptom and describes solutions to those problems.
Troubleshooting Serial Line Problems

Table 6-14 Modem Cannot Send or Receive Data

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
</table>
| Modem speed setting is not locked | • Enter the show line 1 privileged EXEC command on the router. The output for the serial port should indicate the currently configured transmit (Tx) and receive (Rx) speeds.  
  • If the line is not configured to the correct speed, use the speed command in asynchronous line configuration mode to set the speed on the router line. Set the value to the highest speed in common between the modem and the router port. If for some reason you cannot use flow control, limit the line speed to 9600 bps. Faster speeds are likely to result in lost data.  
  • Use the show line 1 command again, and confirm that the line speed is set to the desired value.  
  • When you are certain that the router line is configured for the desired speed, initiate a reverse Telnet session to the modem on that line.  
  • Use a modem command string that includes the lock DTE speed command for your modem. See your modem documentation for exact configuration command syntax.  
The lock DTE speed command, which might also be referred to as port rate adjust or buffered mode, is often related to the way in which the modem handles error correction. This command varies widely between modems.  
Locking the modem speed ensures that the modem always communicates with the Cisco router at the speed configured on the Cisco serial port. If this command is not used, the modem will revert to the speed of the data link (the telephone line) instead of communicating at the speed configured on the router. |
Asynchronous Dial-up Problems

Table 6-14  Modem Cannot Send or Receive Data (continued)

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware flow control not configured on local or remote modem or router</td>
<td>• Enter the show line 0 privileged EXEC command, and look for the following in the Capabilities field:</td>
</tr>
<tr>
<td></td>
<td>Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out...</td>
</tr>
<tr>
<td></td>
<td>If there is no mention of hardware flow control in this field, hardware flow control is not enabled on the line.</td>
</tr>
<tr>
<td></td>
<td>• Configure hardware flow control on the line using the flowcontrol hardware command in asynchronous line configuration mode. If for some reason you cannot use flow control, limit the line speed to 9600 bps. Faster speeds are likely to result in lost data.</td>
</tr>
<tr>
<td></td>
<td>• After enabling hardware flow control on the router line, initiate a reverse Telnet session to the modem via that line.</td>
</tr>
<tr>
<td></td>
<td>• Use a modem command string that includes the RTS/CTS Flow command for your modem. This command ensures that the modem is using the same method of flow control (that is, hardware flow control) as the Cisco router. See your modem documentation for exact configuration command syntax.</td>
</tr>
<tr>
<td>Problem with dialing modem</td>
<td>Make sure that the dialing modem is operational and is securely connected to the correct port. See if another modem works when connected to the same port.</td>
</tr>
</tbody>
</table>

Modem Cannot Send or Receive IP Data

**Symptom:** After a dial-up connection is established, a modem cannot send or receive IP data.

**Note**  For general problems associated with a modem that cannot send or receive data, refer to the section “Modem Cannot Send or Receive Data” earlier in this chapter.

Table 6-15 outlines the problems that might cause this symptom and describes solutions to those problems.
## Troubleshooting Serial Line Problems

### Table 6-15  Modem Cannot Send or Receive IP Data

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP routing not enabled on local or remote router</td>
<td>Make sure that IP routing is enabled on the local and remote routers. For information on enabling IP routing, refer to either Chapter 3, “Configuring Remote Office to Corporate Office Networks” or Chapter 4, “Configuring Small Office to ISP Networks.”</td>
</tr>
</tbody>
</table>
| No default gateway specified on PC                    | • Enter the `show slip` privileged EXEC command. Make sure that the specified IP address is the same as the default gateway specification on the PC.  
• Check the specified default gateway address on the PC. If the IP address is not correct, specify the correct address. For instructions on verifying and changing the default gateway address on the workstation, refer to the vendor documentation. |
| Hardware flow control not configured on local or remote modem or router | • Enter the `show line 0` privileged EXEC command, and look for the following in the Capabilities field: 
  
  `Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out...`
  
  If there is no mention of hardware flow control in this field, hardware flow control is not enabled on the line.  
• Configure hardware flow control on the line using the `flowcontrol hardware` command in asynchronous line configuration mode. If for some reason you cannot use flow control, limit the line speed to 9600 bps. Faster speeds are likely to result in lost data.  
• After enabling hardware flow control on the router line, initiate a reverse Telnet session to the modem via that line.  
• Use a modem command string that includes the RTS/CTS Flow command for your modem. This command ensures that the modem is using the same method of flow control (that is, hardware flow control) as the Cisco router. See your modem documentation for exact configuration command syntax. |
| Static routes not configured                           | • Use the `show ip route` privileged EXEC command to see if there is a static route to the remote network in the routing table.  
• If there is not a static route to the remote network, configure one using the `ip route` command. The static route should point to the remote network. |
Asynchronous Dial-up Problems

Table 6-15 Modem Cannot Send or Receive IP Data (continued)

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
</table>
| Domain Name System (DNS) server not specified on router or workstation | • Check to see if the workstation and router both have DNS information specified. On the router, use the `show running-config` privileged EXEC command to see if DNS is configured. For information on verifying the workstation configuration, refer to the vendor documentation.  
  • If the router and workstation are not configured to use DNS, use the `ip domain-lookup`, `ip domain-name`, and `ip name-server` commands to configure the router.  
  Configure a DNS server address in the TCP/IP software on the PC. For more information, refer to the vendor documentation. |

Modem Cannot Send or Receive IPX Data

**Symptom:** After a dial-up connection is established, a modem cannot send or receive Novell IPX data.

**Note** For general problems associated with a modem that cannot send or receive data, refer to the section “Modem Cannot Send or Receive Data” earlier in this chapter.
Table 6-16 outlines the problems that might cause this symptom and describes solutions to those problems.

**Table 6-16  Modem Cannot Send or Receive IPX Data**

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPX not enabled on the router</td>
<td>Make sure that IPX routing is enabled on the router. For information on configuring IPX routing, refer to Chapter 3, “Configuring Remote Office to Corporate Office Networks.”</td>
</tr>
</tbody>
</table>
| Incorrect Ethernet encapsulation | • Enter the `show ipx servers` privileged EXEC command on your router. If the router is not in the listing, the Ethernet encapsulation might be incorrect.  
• Configure the correct Ethernet encapsulation by using the `ipx network encapsulation encapsulation-type` command in Ethernet interface configuration mode. The encapsulation must be the same as that for your server. |

**Modem Does Not Disconnect Properly**

**Symptom:** Modem does not disconnect properly. Connections to the modem do not terminate when the `quit` command is entered.

Table 6-17 outlines the problems that might cause this symptom and describes solutions to those problems.

**Table 6-17  Modem Does Not Disconnect Properly**

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modem is not sensing DTR</td>
<td>Enter the Hangup DTR modem command string. This command tells the modem to drop carrier when the DTR signal is no longer being received. For the exact syntax of this command, see your modem documentation.</td>
</tr>
</tbody>
</table>
| Modem control is not enabled on the router | • Use the `show line 1` privileged EXEC command on the router. The output should show `inout` or `RIisCD` in the Modem column, which indicates that modem control is enabled on the line of the router.  
• If necessary, configure modem control by using the `modem inout` command in asynchronous line configuration mode. |
Asynchronous Dial-up Problems

Link Goes Deactivates Soon

**Symptom:** After a dial-up connection is established, the link deactivates too quickly.

Table 6-18 outlines the problems that might cause this symptom and describes solutions to those problems.

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
</table>
| Dialer timeout is too short | • Use the `show running-config` privileged EXEC command to view the router configuration. Check the value configured with the `dialer idle-timeout` command.  
  • Increase the timeout value using the `dialer idle-timeout seconds` command. The default is 120 seconds. |
| Dialer lists are too restrictive | • Use the `show running-config` privileged EXEC command to view the router configuration. Check the access lists, if any, referenced by `dialer list` commands.  
  • Make sure the access lists describe all the traffic that should keep the link active. Reconfigure the access lists to include additional traffic if necessary. |
Troubleshooting Serial Line Problems

Link Does Not Deactivate or Stays Activated Too Long

**Symptom:** After a dial-up connection is established, the link activates indefinitely or stays activated too long in an idle state.

Table 6-19 outlines the problems that might cause this symptom and describes solutions to those problems.

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dialer lists not restrictive enough</td>
<td>• Use the <code>show running-config</code> privileged EXEC command to view the router configuration. Check the access lists, if any, referenced by <code>dialer list</code> commands.</td>
</tr>
<tr>
<td></td>
<td>• Make sure the access lists do not describe traffic that should not keep the link active. Reconfigure the access lists if necessary.</td>
</tr>
<tr>
<td>Modems misconfigured</td>
<td>Make sure the local and remote modems are properly configured. In particular, both modems should be configured to disconnect on loss of DTR (Hangup DTR). For the exact syntax of this command, see your modem documentation.</td>
</tr>
</tbody>
</table>
Poor Performance

**Symptom:** After a dial-up connection is established, performance over the link is slow or unreliable, often due to a high rate of data loss.

Table 6-20 outlines the problems that might cause this symptom and describes solutions to those problems.

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error correction is not configured on the modem</td>
<td>Make certain the modem is configured for error correction. For the exact syntax of the command, see your modem documentation.</td>
</tr>
</tbody>
</table>
| Flow control is not enabled, is enabled only on one device (either DTE or DCE), or is misconfigured | - Enter the `show line 0` privileged EXEC command, and look for the following in the Capabilities field:  
  ```cap
  Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out...
  ```  
  If there is no mention of hardware flow control in this field, hardware flow control is not enabled on the line.  
  - Configure hardware flow control on the line using the `flowcontrol hardware` command in asynchronous line configuration mode. If for some reason you cannot use flow control, limit the line speed to 9600 bps. Faster speeds are likely to result in lost data.  
  - After enabling hardware flow control on the router line, initiate a reverse Telnet session to the modem via that line.  
  - Use a modem command string that includes the RTS/CTS Flow command for your modem. This command ensures that the modem is using the same method of flow control (that is, hardware flow control) as the Cisco router. See your modem documentation for exact configuration command syntax. |
| Congestion or line noise            | - If the network is congested, dial-up connections can freeze for a few seconds. The only solution is to reduce congestion on the network by increasing bandwidth or redesigning the network.  
  - Line noise can also freeze up a dial-up connection. For information on how to account for line noise for your modem, refer to the vendor documentation. |
Frame Relay Problems

This section describes how to troubleshoot the following Frame Relay symptoms:

- Frame Relay Link is Down
- Cannot Ping Remote Router
- Cannot Ping End to End

Frame Relay Link is Down

**Symptom:** Connections over a Frame Relay link fail.

Table 6-21 outlines the problems that might cause this symptom and describes solutions to those problems.

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cabling, hardware, or carrier problem</td>
<td>Perform these steps on the local and remote routers.</td>
</tr>
<tr>
<td></td>
<td>Use the <strong>show interfaces serial 0</strong> command to see if the interface and line protocol are up.</td>
</tr>
<tr>
<td></td>
<td>If the interface and line protocol are down, refer to the <em>Cisco 805 Router Hardware Installation Guide</em> to confirm that you are using the correct serial cable to connect the CSU/DSU and that you connected the CSU/DSU correctly. Make sure cables are securely attached.</td>
</tr>
<tr>
<td></td>
<td>If the cable is correct, try moving it to a different port. If that port works, then the first port is defective. Replace the router.</td>
</tr>
<tr>
<td></td>
<td>If the cable does not work on the second port, replace the cable. If it still does not work, there might be a problem with the DCE. Contact your carrier about the problem.</td>
</tr>
</tbody>
</table>
Frame Relay Problems

Table 6-21  Frame Relay Link is Down (continued)

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>LMI type mismatch</td>
<td>• Use the show interfaces serial 0 command to check the state of the interface.</td>
</tr>
<tr>
<td></td>
<td>• If the output shows the interface is up but the line protocol is down, enter the show frame-relay lmi privileged EXEC command to see which LMI type is configured on the Frame Relay interface.</td>
</tr>
<tr>
<td></td>
<td>• Make sure that the LMI type is the same for all devices in the path from source to destination. Enter the frame-relay lmi-type {ansi</td>
</tr>
<tr>
<td>Keepalives not being sent</td>
<td>• Enter the show interfaces serial 0 command to find out if keepalives are configured. If you see a line that says “keepalives not set,” keepalives are not configured.</td>
</tr>
<tr>
<td></td>
<td>• Use the keepalive seconds command in serial interface configuration mode to configure keepalives. The default value for this command is 10 seconds.</td>
</tr>
<tr>
<td>Encapsulation mismatch</td>
<td>• When connecting Cisco devices with non-Cisco devices, you must use IETF encapsulation on both devices. Check the encapsulation type on the Cisco device by using the show frame-relay map privileged EXEC command.</td>
</tr>
<tr>
<td></td>
<td>• If the Cisco device is not using IETF encapsulation, use the encapsulation frame-relay ietf command in serial interface configuration mode to configure IETF encapsulation on the Cisco Frame Relay interface. For information on viewing or changing the configuration of the non-Cisco device, refer to the vendor documentation.</td>
</tr>
</tbody>
</table>
Troubleshooting Serial Line Problems

Cannot Ping Remote Router

**Symptom:** Attempts to ping the remote router across a Frame Relay connection fail.

Table 6-22 outlines the problems that might cause this symptom and describes solutions to those problems.

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
</table>
| Encapsulation mismatch            | - When connecting Cisco devices with non-Cisco devices, you must use IETF encapsulation on both devices. Check the encapsulation type on the Cisco device by using the `show frame-relay map` privileged EXEC command.  
  - If the Cisco device is not using IETF encapsulation, use the `encapsulation frame-relay ietf` command in serial interface configuration mode to configure IETF encapsulation on the Cisco Frame Relay interface. For information on viewing or changing the configuration of the non-Cisco device, refer to the vendor documentation. |
Frame Relay Problems

### Table 6-22 Cannot Ping Remote Router (continued)

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
</table>
| DLCI inactive or deleted     | • Enter the `show frame-relay pvc` privileged EXEC command to view the status of the interface PVC.  
                               |   • If the output shows that the PVC is inactive or deleted, there is a problem along the path to the remote router. Check the remote router or contact your carrier to check the status of the PVC. |
| DLCI assigned to wrong       | • Use the `show frame-relay pvc` privileged EXEC command to check the assigned DLCIs. Make sure that the correct DLCIs are assigned to the correct subinterface.  
                               |   • If the DLCIs appear to be correct, shut down the main interface by entering the `shutdown` command in serial interface configuration mode, then bring the interface back up entering the `no shutdown` command. |
| subinterface                 |                                                                          |
| Misconfigured access list    | • Enter the `show access-list` privileged EXEC command to see if there are access lists configured on the router.  
                               |   • If there are access lists configured, test connectivity by disabling access lists by entering the `no access-group` command in global configuration mode. Check to see if connectivity is restored.  
                               |   • If connections work, reenable access lists one at a time, checking connections after enabling each access list.  
                               |   • If enabling an access list blocks connections, make sure that the access list does not deny necessary traffic. Make sure to configure explicit `permit` statements for any traffic you want to pass.  
                               |   • Continue testing access lists until all access lists are restored and connections still work. |
Troubleshooting Serial Line Problems

Table 6-22 Cannot Ping Remote Router (continued)

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>frame-relay map</strong> command missing</td>
<td>• Enter the <code>show frame-relay map</code> privileged EXEC command to see if an address map is configured for the DLCI.</td>
</tr>
<tr>
<td></td>
<td>• If you do not see an address map for the DLCI, enter the <code>clear frame-relay-inarp</code> privileged EXEC command and then enter the <code>show frame-relay map</code> command again to see if there is now a map to DLCI.</td>
</tr>
<tr>
<td></td>
<td>• If there is no map to the DLCI, add a static address map by entering the <code>frame-relay map</code> command in serial interface configuration mode. For complete information on configuring Frame Relay address maps, refer to the <em>Cisco IOS Wide-Area Networking Configuration Guide</em> publication.</td>
</tr>
<tr>
<td></td>
<td>• Make sure that the DLCIs and next-hop addresses specified in <code>frame-relay map</code> commands are correct. The specified protocol address should be in the same network as your local Frame Relay interface.</td>
</tr>
</tbody>
</table>

| No broadcast keyword in `frame-relay map` statements | • Enter the `show running-config` privileged EXEC command on the local and remote routers to view the router configuration. Check `frame-relay map` command entries to see if the broadcast keyword is specified. |
|                                                      | • If the keyword is not specified, add the broadcast keyword to all `frame-relay map` commands. By default, the broadcast keyword is added to dynamic maps learned via Inverse ARP. |

1 You can eliminate the need for static Frame Relay address maps by using Inverse ARP instead. Use the `frame-relay interface-dlci dlci broadcast` interface configuration command to configure an interface to use Inverse ARP. For more information about the use of this command, refer to the *Cisco IOS Wide-Area Networking Configuration Guide* and *Wide-Area Networking Command Reference*.

Cannot Ping End to End

**Symptom:** Attempts to ping devices on a remote network across a Frame Relay connection fail.

Table 6-23 outlines the problems that might cause this symptom and describes solutions to those problems.
This section describes how to troubleshoot the following X.25 symptoms:

- No Connections over X.25 Link
- Excess Serial Errors on X.25 Link

### No Connections over X.25 Link

**Symptom:** Connections over an X.25 link fail.

Table 6-24 outlines the problems that might cause this symptom and describes solutions to those problems.
### Troubleshooting Serial Line Problems

#### Table 6-24  No Connections over X.25 Link

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
</table>
| Incorrect cabling or bad router hardware      | • Check all cabling and hardware for damage or wear. Replace cabling or hardware as required. For more information on the Cisco 805 router and serial cables, refer to the [Cisco 805 Router Hardware Installation Guide](#).  
• Enter the `show interfaces serial 0` privileged EXEC command to determine the status of the interface.  
• If the interface is down, refer to the “Serial Connection” section earlier in this chapter. If the interface is up but the line protocol is down, check the (Link Access Procedure, Balanced) LAPB state in the output of the `show interfaces serial 0` command.  
• If the LAPB state is not CONNECT, use the `debug lapb` privileged EXEC command (or attach a serial analyzer) to look for set asynchronous balance mode requests (SABMs) being sent, and for UA packets being sent in reply to SABMs. If UAs are not being sent, one of the other possible problems described in this table is the likely cause.  
• If the `show interfaces serial 0` command indicates that the interface and line protocol are up but no connections can be made, there is probably a router or switch misconfiguration. Refer to the other possible problems outlined in this table.  
| Link is down                                  | Enter the `show interfaces serial 0` privileged EXEC command to determine if the link is down. If the link is down, refer to the “Serial Connection” section earlier in this chapter.  
| Misconfigured protocol parameters             | • Enable the `debug lapb` privileged EXEC command and look for SABMs being sent. If no SABMs are being sent, disable the `debug lapb` command and enable the `debug x25 events` privileged EXEC command.  
• Look for `RESTART` messages (for PVCs) or `CLEAR REQUESTS` with non-zero cause codes (for SVCs). To interpret X.25 cause and diagnostic codes provided in the `debug x25 events` output, refer to the [Debug Command Reference](#) document.  
• Verify that all critical LAPB parameters (modulo, T1, N1, N2, and k) and the critical X.25 parameters (modulo, X.121 addresses, SVC ranges, PVC definitions, and default window and packet sizes) match the parameters required by the X.25 service provider. |
Excess Serial Errors on X.25 Link

Symptom: The output of the `show interfaces serial 0` privileged EXEC command shows rejects (REJs), receiver not ready events (RNRs), protocol frame errors (FRMRs), restarts (RESTARTs), or disconnects (DISCs) in excess of 0.5 percent of information frames (IFRAMEs).

Note: If any of these fields are increasing and represent more than 0.5 percent of the number of IFRAMEs, there is probably a problem somewhere in the X.25 network. There should always be at least one SABM. However, if there are more than 10, the packet switch probably is not responding.

Table 6-25 outlines the problem that might cause this symptom and describes solutions to this problem.
Using Debug Commands

You can use the debug commands to troubleshoot any configuration problems on your network. Debug commands provide extensive, informative displays to help you interpret any problems.

The following list contains important information about 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 and few users to decrease the likelihood that the debug command processing overhead affects network users.

---

### Table 6-25 No Connections over X.25 Link

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
</table>
| Incorrect cabling or bad router hardware | - Check all cabling and hardware for damage or wear. Replace cabling or hardware as required. For more information on the Cisco 805 router and serial cables, refer to the *Cisco 805 Router Hardware Installation Guide*.  
  - Enter the `show interfaces serial 0` privileged EXEC command to determine the status of the interface.  
  - If the interface is down, refer to the “Serial Connection” section earlier in this chapter. If the interface is up but the line protocol is down, check the LAPB (Link Access Procedure, Balanced) state in the output of the `show interfaces serial 0` command.  
  - If the LAPB state is not CONNECT, use the `debug lapb` privileged EXEC command (or attach a serial analyzer) to look for set asynchronous balance mode requests (SABMs) being sent, and for UA packets being sent in reply to SABMs. If UAs are not being sent, one of the other possible problems described in this table is the likely cause.  
  - If the `show interfaces serial 0` command indicates that the interface and line protocol are up but no connections can be made, there is probably a router or switch misconfiguration. Refer to the other possible problems outlined in this table. |
You can find additional information and documentation about the debug commands in the Debug Command Reference document on the Documentation CD-ROM that came with your router.

To turn off any debugging, enter the `undebug all` command.

If you want to use a debug command during a Telnet session with your router, you must first enter the `terminal monitor` command.
Using Debug Commands
This appendix describes the Cisco 805 router ROM monitor. The ROM monitor runs when the router is powered up or reset and helps to initialize the processor hardware and boot the operating system software.

You might need to access the ROM monitor for the following reasons:

- To reconfigure certain basic configuration parameters, such as the baud rate of the console port
- To set up your router to boot from a TFTP server on an Ethernet network (rather than to boot from Flash memory, which is the default)

To use the ROM monitor, you must connect a terminal or PC to the light-blue console port on the router. (For information on making this connection, see the Cisco 805 Router Hardware Installation Guide.)

Using ROM Monitor

To use the ROM monitor, perform the following steps:

**Step 1** Determine whether the Flash memory contains a software image or not.

The Flash memory contains a software image unless you deleted it by using the ROM monitor `erase` command.
ROM Monitor Modes

Step 2  Reload the software by doing one of the following:

  - Enter the following command in privileged EXEC mode:

    ```
    router# reload
    ```

  - Turn the router to STANDBY, wait 5 seconds, and then turn it to ON again.

Step 3  Perform this step only if Flash memory contains a software image. Before the terminal or PC displays `Boot...,...`(approximately 10 seconds), press Escape, Control-C, or Break.

The router enters the ROM monitor as indicated by the following prompt:

```
boot#
```

While in the ROM monitor, you can access basic configuration parameters and commands. The parameters and commands that you can access depends on the mode you are in. For more information on modes, see the next section. For information on parameters, see the “Configuring Basic Configuration Parameters” section later in this appendix. For information on commands, see the “Commands” section later in this appendix.

ROM Monitor Modes

The ROM monitor consists of the following modes:

  - Enable—You can set all parameters and issue all commands in enable mode. By default, you are in enable mode when you enter the ROM monitor (`boot #`).

  - Disable—You can set a small subset of parameters and issue a small subset commands in disable mode. If you set up a ROM monitor password, you are in disable mode when you enter the ROM monitor (`boot `).

Note  Cisco does not recommend setting a ROM monitor password. The only situation in which you should set a password is if you allow remote access via a modem to the ROM monitor. If you set this password, you will be in disable mode when you enter the ROM monitor and must enter the password if you want to enter enable mode. If you forget this password, you must contact the Cisco Technical Assistance Center to recover it.
You can access these modes by entering the following commands at the ROM monitor prompt:

- To access enable mode, enter the `enable` command.
- To access disable mode, enter the `disable` command.

The parameters and commands that you can access depends on the mode you are in. For more information on parameters, commands, and modes, see the “Configuring Basic Configuration Parameters” section and the “Commands” section later in this appendix.

### Configuring Basic Configuration Parameters

To access a listing of the basic configuration parameters and their possible settings, enter the following command:

```
boot# set ?
```

A display similar to the following appears:

```
set baud={300|1200|2400|4800|9600|19200|38400|57600|115200}
set data-bits={7|8}
set parity={none|even|odd}
set stop-bits={1|2}
set console-flags={rts|dsr}
set mac-address=X.X.X
set unit-ip=N.N.N.N
set serv-ip=N.N.N.N
set netmask=N.N.N.N
set gate-ip=N.N.N.N
set pkt-timeout=N (seconds)
set tftp-timeout=N (seconds)
set boot-action={flash|tftp|none}
set debug-flags=N
set file-name="file-name"
set watchdog={off|on}
set prompt="prompt-string"
set ios-conf=N
```
Configuring Basic Configuration Parameters

Note  This display shows all available parameters. The parameters that actually display depends on which mode you are in. For information on modes, see the “ROM Monitor Modes” section earlier in this appendix.

To configure a parameter, use the following command at the ROM monitor prompt:

```
set parameter=value
```

For example, to set the baud rate parameter to 19200, enter the following:

```
boot# set baud=19200
```

Table A-1 describes the parameters, their defaults, and which modes they can be configured in.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
<th>Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>baud&lt;sup&gt;1&lt;/sup&gt;</td>
<td>Baud rate of console port.</td>
<td>9600</td>
<td>enable</td>
</tr>
<tr>
<td>data-bits&lt;sup&gt;1&lt;/sup&gt;</td>
<td>Data bits of console port.</td>
<td>8</td>
<td>enable</td>
</tr>
<tr>
<td>parity&lt;sup&gt;1&lt;/sup&gt;</td>
<td>Parity of console port.</td>
<td>–</td>
<td>enable</td>
</tr>
<tr>
<td>stop-bits&lt;sup&gt;1&lt;/sup&gt;</td>
<td>Stop bits of console port.</td>
<td>1</td>
<td>enable</td>
</tr>
<tr>
<td>console-flags&lt;sup&gt;1&lt;/sup&gt;</td>
<td>Flags for console port.</td>
<td>0</td>
<td>enable</td>
</tr>
<tr>
<td>mac-address</td>
<td>Ethernet MAC address for your router, such as 0BAD.1BAD.2BAD.</td>
<td>xxxxx.xxx x.xxxx (Factory sets this value.)</td>
<td>enable</td>
</tr>
<tr>
<td>unit-ip</td>
<td>IP address of your router.</td>
<td>0.0.0.0</td>
<td>enable</td>
</tr>
</tbody>
</table>

<sup>1</sup> Enter 1 for rts, 2 for dsr, or 3 for both.
### Table A-1 Basic Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
<th>Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>serv-ip</td>
<td>IP address of your TFTP server. Used only if router is set up to boot from a TFTP server on your network.</td>
<td>0.0.0.0</td>
<td>enable</td>
</tr>
<tr>
<td>netmask</td>
<td>Subnet mask for IP address.</td>
<td>0.0.0.0</td>
<td>enable</td>
</tr>
<tr>
<td>gate-ip</td>
<td>Default gateway IP address. Used only if router is set up to boot from a TFTP server and if the server is on a different subnet.</td>
<td>0.0.0.0</td>
<td>enable</td>
</tr>
<tr>
<td>pkt-timeout</td>
<td>Number of seconds before router retries a TFTP ACK or RRQ.</td>
<td>4</td>
<td>enable</td>
</tr>
<tr>
<td>tftp-timeout</td>
<td>Number of seconds before TFTP ACK or RRQ fails.</td>
<td>16</td>
<td>enable</td>
</tr>
<tr>
<td>boot-action</td>
<td>Action that router takes on power up:</td>
<td>flash</td>
<td>enable</td>
</tr>
<tr>
<td>file-name</td>
<td>Action that router takes on power up:</td>
<td>c805-y6-mw</td>
<td>enable</td>
</tr>
<tr>
<td>watchdog$^2$</td>
<td>Automatic reboot if router becomes nonfunctional.</td>
<td>on</td>
<td>enable</td>
</tr>
<tr>
<td>prompt</td>
<td>CLI prompt string.</td>
<td>boot #</td>
<td>disable, enable</td>
</tr>
<tr>
<td>ios-conf</td>
<td>Reset the configuration register. Equivalent to <code>config-register</code> software command.</td>
<td>0</td>
<td>enable</td>
</tr>
</tbody>
</table>

1. Reset the console port to recognize the new setting of this parameter by using the `reset` command.
2. Save this configuration, then turn the power to standby, and then on again for this new setting to take effect.
3. This parameter is not currently supported.
To access a listing of the ROM monitor commands and a brief description of each command, enter the following command:

```
boot# help
```

A display similar to the following appears:

- **boot**: Execute image or CLI command script.
- **delete**: Deletes file-name from flash (8th delete is permanent).
- **disable**: Disable privileged commands.
- **echo**: Display arguments (to test CLI behavior).
- **enable**: Enable privileged or debug commands.
- **flash**: Single cycle id/erase/write test for each flash chip.
- **help**: Display help for command (* for all).
- **list**: List files currently in ram and saved in flash.
- **load**: Load saved boot environment from flash.
- **passwd**: Set or change the ROM password.
- **reset**: Reset console port to current parameters.
- **set**: Set boot environment values.
- **save**: Save boot environment or loaded file to flash.
- **show**: Show current or saved boot environment.
- **test**: Initiate endless H/W bringup testing.
- **upload**: Load image or configuration data into RAM.
- **undelete**: Undelete file-name (maximum of 8 deletes & undeletes).

**Note**: This display shows all available commands. The commands that actually display depend on which mode you are in. For information on modes, see the “ROM Monitor Modes” section earlier in this appendix.

Table A-2 describes the commands and which modes they can be used in.
### Table A-2  ROM Monitor Commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot [flash</td>
<td>By default, router boots a loaded file if present. If you specify flash, router executes file stored in Flash memory. If you specify tftp, router loads TFTP file (image or script) and executes it.</td>
<td>enable</td>
</tr>
<tr>
<td>= filename]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>delete filename</td>
<td>Marks specified filename as deleted from Flash memory. (You need to specify pathname as well as filename.) The eighth time you delete a specified filename, the file is permanently deleted.</td>
<td>enable</td>
</tr>
<tr>
<td>disable</td>
<td>Enter disable mode, which has access to fewer parameters and commands than enable mode.</td>
<td>disable, enable</td>
</tr>
<tr>
<td>echo [arguments]</td>
<td>Display arguments to test the CLI.</td>
<td>enable</td>
</tr>
<tr>
<td>enable</td>
<td>Enter enable mode.</td>
<td>disable, enable</td>
</tr>
<tr>
<td>erase</td>
<td>Erases files marked for deletion from Flash memory.</td>
<td>enable</td>
</tr>
<tr>
<td>help [command</td>
<td>• Enter <strong>help</strong> or <strong>help</strong> * to display a brief description of each available command. • Enter <strong>help</strong> command to display a brief description of a particular command.</td>
<td>disable, enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>list</td>
<td>List files currently in RAM and saved in Flash memory.</td>
<td>disable, enable</td>
</tr>
<tr>
<td>load</td>
<td>Load current software configuration stored in Flash memory.</td>
<td>disable, enable</td>
</tr>
<tr>
<td>passwd</td>
<td>Set or change the ROM monitor password, which protects the enable-mode commands. Cisco recommends setting up this password only if you allow remote access to the ROM monitor. If you set up a password, you will enter the disable mode in the ROM monitor and must enter the password if you want to enter the enable mode. If you forget the password, you must contact the Cisco Technical Assistance Center to recover it.</td>
<td>enable</td>
</tr>
</tbody>
</table>
### Commands

**Table A-2 ROM Monitor Commands (continued)**

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>reboot</td>
<td>Resets the hardware, and boots the software.</td>
<td>enable</td>
</tr>
<tr>
<td>reset</td>
<td>Reset console port to recognize reconfigured parameters.</td>
<td>enable</td>
</tr>
</tbody>
</table>

**save [file [= file-name]]**
- Enter `save` to save current configuration to Flash memory.  
- Enter `save file` to save loaded file to Flash memory as the current filename.  
- Enter `save file=filename` to save loaded file to Flash memory as the specified filename.  
- Enter `list` to determine filename.

**set [variable={value | ?}] [? [variables | *]]**
- Enter `set` to display all parameters and their current values.  
- Enter `set ?` to display all parameters and their possible values.  
- Enter `set ? variable` to display a description of a particular parameter and its possible values or `set ? *` to display a description of all available parameters and their possible values.  
- Enter `set variable=value` to configure a parameter. Enter `set variable=?` to display a description of the specified parameter and its possible values.

**show [saved]**
- Show current or saved configuration.  

**upload [serial | tftp | xmodem] [= filename]**
- Load software image or configuration data from the specified source into RAM.

**undelete [filename]**
- Undo the deletion of specified filename up to eight times.
Booting from a TFTP Server

Before setting up your router to boot from a TFTP server, you must understand that booting from a TFTP server consumes more dynamic RAM (DRAM) than booting from Flash memory. The amount of DRAM lost is equivalent to the software image size and is displayed when the router boots.

To set up your router to boot from a TFTP server that is on an Ethernet network, follow these steps:

Step 1  Set IP addresses for the router and the TFTP server by entering the following commands:

```plaintext
set unit-ip=ip-address
set serv-ip=ip-address
```

Step 2  Set up the subnet mask by entering the following command:

```plaintext
set netmask=subnet-mask
```

Step 3  If the TFTP server is on a different subnet than the router, set up an IP address for a gateway server by entering the following command:

```plaintext
set gate-ip=ip-address
```

Step 4  Set up the filename for the software image or script that will reside on the TFTP server by entering the following command:

```plaintext
set file-name=filename
```

Your TFTP server configuration determines the filename.

Step 5  Boot the software by using one of the following methods:

(a) If you want to set up the router to boot from the TFTP server each time you power-on the router, enter the following command:

```plaintext
boot# set boot-action=tftp
```

Save the current configuration to Flash memory by entering the `save` command. Turn the power to STANDBY and then to ON again.
(b) If you want to boot from the TFTP server now but not each time you
power-on the router, enter the following command:

```bash
boot# boot tftp=[filename]
```
Upgrading the Software

You can upgrade your software in the following ways:

- From the Cisco IOS command-line interface (CLI)
- From the ROM monitor

Cisco recommends upgrading your software from the CLI for the following reasons:

- You can leave your router running during the software upgrade, but if you upgrade from the ROM monitor, you have to power down your router.
- Your overall software upgrade time is shorter if you use the CLI than if you upgrade from the ROM monitor. (The software upgrade time from the CLI can vary depending on the amount of activity on the link and whether the Trivial File Transfer Protocol [TFTP] server is local or remote.)

To upgrade your software from the CLI, you need a Cisco 805 router that is running Cisco IOS software and a TFTP server.

Upgrading Software from the CLI

Follow these steps to upgrade the software:

**Step 1** To download a current Cisco IOS release, go to the following URL. This URL is subject to change without notice.

http://www.cisco.com/cgi-bin/ibld/all.pl?i=support&c=3

The Service and Support window is displayed.
Step 2  Follow this path:

Cisco IOS Software: Cisco IOS Release release_number: Download Cisco IOS Software

Step 3  Select the appropriate information in each section of the Cisco IOS Planner window.
• Platform
• Release
• Software feature

Step 4  Transfer the software release to your TFTP server.

The download of software from the TFTP server to the router can occur through either the router Ethernet or serial port. You can initiate a session with the TFTP server through either the console port or a Telnet session.

Step 5  Modify Flash memory so that you can load your new software image in Flash memory and yet the run the old image:

router# erase flash

Step 6  From the privileged EXEC mode, download the software from the TFTP server:

router# copy tftp://ip/filename flash:filename

ip is either the IP address of the TFTP server or if you have the domain name system (DNS) set up, the name of the TFTP server.

Step 7  Enter global configuration mode:

router# configure
router(config)#

Step 8  Specify the image that the router loads at startup:

router(config)# boot system flash filename

filename is the file stored in Flash memory that you specified in Step 6.
Upgrading Software from ROM Monitor

Upgrading Software from ROM Monitor

Follow these steps to upgrade your software:

Step 1  To download a current Cisco IOS release, go to the following URL. This URL is subject to change without notice.

   http://www.cisco.com/kobayashi/sw-center

   The Software Center window is displayed.

Step 2  Follow this path:

   Cisco IOS Software: Cisco IOS Release release_number: Download Cisco IOS Software

Step 3  Select the appropriate information in each section of the Cisco IOS Planner window.
   • Platform
   • Release
   • Software feature

Transfer the software release to one of the sources described in Table B-1.

Exit to privileged EXEC mode:

   router(config)# exit
   router#

Step 9  Save your configuration changes to nonvolatile RAM (NVRAM):

   router# copy running-config startup-config

Step 10 Reload the operating system:

   router# reload
Step 4 Enter the ROM monitor by performing the following steps:

(a) Reload the software by doing one of the following:

- Enter the following command from privileged EXEC mode:
  
  `router# reload`

- Turn the router to STANDBY, wait 5 seconds, and then turn it to ON again.

(b) Immediately press *Escape*, *Control-C*, or *Break*.

  The router enters the ROM monitor as indicated by the following prompt:

  `boot#`

Step 5 Set up a default filename for the software image:

  `boot# set file-name=filename`

Step 6 Download your software.

  Follow the procedure in the “Downloading Software from a TFTP Server” section or in the “Downloading Software from a Host Running XMODEM and a Terminal Emulator” section later in this appendix.

---

**Table B-1 Software Image Download Sources**

<table>
<thead>
<tr>
<th>Source</th>
<th>Source Connection to Router</th>
</tr>
</thead>
<tbody>
<tr>
<td>TFTP server</td>
<td>Data passes through Ethernet or serial port. Session is initiated through console port or Telnet session.</td>
</tr>
<tr>
<td>Host running the XMODEM protocol and terminal emulation software such as HyperTerm.¹</td>
<td>Router console port.</td>
</tr>
</tbody>
</table>

¹ For information on terminal emulation software and the appropriate console settings so that the host and router can communicate, refer to Chapter 2, “Cisco IOS Basic Skills.”
Upgrading Software from ROM Monitor

Downloading Software from a TFTP Server

The following procedure describes how to download software from a TFTP server. This procedure uses the following sample network:

- Cisco 805 router with an IP address of 10.1.0.1 and a subnet mask of 255.255.255.0
- TFTP server with an IP address of 10.2.0.2
- Gateway server with an IP address of 10.1.0.2

**Step 1**  Set IP address for the TFTP server:

```
boot# set serv-ip = 10.2.0.2
```

**Step 2**  Set IP address and subnet mask for the router:

```
boot# set unit-ip = 10.1.0.1
boot# set netmask = 255.255.255.0
```

**Step 3**  If the TFTP server is on a different subnet than the router, set up an IP address for a gateway server:

```
boot# set gate-ip = 10.1.0.2
```

**Step 4**  Download the software image from the TFTP server:

```
boot# upload tftp
```

The following is a sample of output that displays while the software is downloading:

```
TFTP initiated.
File name: c800-g3n-mw
RAM size: 0x00650bc8 (6622152)
Raw size: 0x00541415 (5510228)
Image size: 0x002cbc28 (2931752)
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
upload: succeeded (17 seconds).
```

**Step 5**  Check to make sure that the software image has been downloaded to RAM:

```
boot# list
```
Step 6  Mark the old software image for deletion:
        boot# delete filename

Step 7  Delete the old software image:
        boot# erase

Step 8  Save the new software image to Flash memory:
        boot# save file

Step 9  Check to make sure that the new software image has been saved to Flash
        memory:
        boot# list

Step 10 Boot the new software image:
        boot# boot flash

Downloading Software from a Host Running XMODEM and a Terminal Emulator

The following procedure describes how to download software from a host running
XMODEM and a terminal emulator.

Step 1  Increase the router console port baud rate:
        boot# set baud=115200

Step 2  Reset the console port:
        boot# reset

Step 3  Optional. If you want the router console port to continue running at 115200
        baud, you can save the configuration:
        boot# save

Step 4  Change your host baud rate to 115200.
        For the new baud rate to take effect, you might need to save the new baud rate,
        exit from the terminal emulator, and reestablish a new session.
Step 5  Download the software image from the host:

    boot# upload xmodem

    The following is a sample of output that displays while the software is
downloading:

    Ready for X/Modem upload...

    [note: no status bar for xmodem transfers,
    abort with Control-X or break]

    upload: succeeded (312 seconds).

Step 6  From your host, enter the XMODEM send command for your terminal
emulation software.

    For example, if you are using HyperTerm, click the Transfer menu and select
Send File. The Send File dialog box appears. Click Browse to locate the
software image. Select XMODEM as the protocol, and click Send.

Step 7  Check to make sure that the software image has been downloaded to RAM:

    boot# list

Step 8  Mark the old software image for deletion:

    boot# delete filename

Step 9  Delete the old software image:

    boot# erase

Step 10  Save the new software image to Flash memory:

    boot# save file

Step 11  Check to make sure that the new software image has been saved to Flash
memory:

    boot# list

Step 12  Boot the new software image:

    boot# boot flash
Downloading Software from a Host Running Only a Terminal Emulator

The following procedure describes how to download software from a host running a terminal emulator but not XMODEM.

**Note** Any failure when using this method is not detected until the software download attempt is complete. (The download attempt can take a significant amount of time.) Because of the potential time lost, Cisco recommends downloading the software from a TFTP server or a host running XMODEM.

**Step 1** Increase the router console port baud rate:

```plaintext
boot# set baud=115200
```

**Step 2** Reset the console port:

```plaintext
boot# reset
```

**Step 3** Optional. If you want the router console port to continue running at 115200 baud, you can save the configuration:

```plaintext
boot# save
```

**Step 4** Change the host baud rate to 115200.

For the new baud rate to take effect, you might need to save the new baud rate, exit from the terminal emulator, and reestablish a new session.

**Step 5** Change the host to **no flow control**.

**Step 6** Download the software image from the host:

```plaintext
boot# upload serial
```
The following is a sample of output that displays while the software is downloading:

Ready for raw ASCII upload...

File name: c800-g3n-mw
RAM size: 0x00650bc8 (6622152)
Raw size: 0x00541455 (5510228)
Image size: 0x002cbc28 (2931752)
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
upload: succeeded (258 seconds).

**Step 7**  On your host, set the interline and intercharacter delays to zero.

**Step 8**  On your host, enter a raw serial upload command to your terminal emulation software.

**Step 9**  Check to make sure that the software image has been downloaded to RAM:

```
boot# list
```

**Step 10**  Mark the old software image for deletion:

```
boot# delete filename
```

**Step 11**  Delete the old software image:

```
boot# erase
```

**Step 12**  Save the new software image to Flash memory:

```
boot# save file
```

**Step 13**  Check to make sure that the new software image has been saved to Flash memory:

```
boot# list
```

**Step 14**  Boot the new software image:

```
boot# boot flash
```
Concepts

This appendix contains information on the following topics:

- IP routing protocols
- Point-to-Point Protocol (PPP) authentication protocols
- Dialer profiles

Selecting IP Routing Protocols

The Cisco 805 router supports the following IP routing protocols:

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

Table C-1 summarizes the characteristics of RIP and EIGRP. The following sections contain more details on RIP and EIGRP.
Selecting IP Routing Protocols

Table C-1  RIP and EIGRP Comparison

<table>
<thead>
<tr>
<th>IP Routing Protocol</th>
<th>Ideal Topology</th>
<th>Metric</th>
<th>Routing Updates</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIP</td>
<td>Suited for topologies with 15 or fewer hops to reach a destination.</td>
<td>Hop count; maximum hop count is 15. Best route is one with lowest hop count.</td>
<td>By default, every 30 seconds. You can reconfigure this value and also use triggered extensions to RIP.</td>
</tr>
<tr>
<td>EIGRP</td>
<td>Suited for large topologies with 16 or more hops to reach a destination.</td>
<td>Distance information. 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.</td>
<td>Hello packets sent every 5 seconds plus incremental updates sent when the state of a destination changes.</td>
</tr>
</tbody>
</table>

Routing Information Protocol

RFC 1058 is the specification for RIP.

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. RIP selects routes based on the lowest hop count. For example, if two routes to the same destination exist and one route has 3 hops associated with it and the other has 2 hops, RIP selects the route with 2 hops. If multiple routes have the same hop count, RIP selects routes alternately. According to RIP, the maximum allowable hop count is 15.

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 data base is updated. For more information on triggered extensions to RIP, refer to the Cisco IOS documentation set. For information on accessing the documentation, see the “References to Cisco IOS Documentation Set” in “About this Guide.”

RIP supports load balancing. You can evenly distribute traffic among multiple routes to the same destination and that have the same metric. By default, the RIP routing table includes up to four equal routes.
Enhanced Interior Gateway Routing Protocol

EIGRP is an advanced Cisco-proprietary distance-vector routing protocol, which means it uses a metric more sophisticated than distance (hop count) for route selection. EIGRP uses a metric 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. If a successor for a particular destination does not exist but neighbors advertise the destination, the router must recompute a route.

Each router running EIGRP sends hello packets every 5 seconds to notify neighboring routers that it is functioning. If a particular router does not send a hello packet within a prescribed period, EIGRP assumes that the state of a destination has changed and sends an incremental update.

Selecting PPP Authentication Protocol

The Cisco 805 router supports two PPP authentication protocols:

- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)

Table C-2 summarizes the characteristics of PAP and CHAP so that you can decide which protocol you want to use. The following sections contain more details on PAP and CHAP.

Note  Cisco recommends using CHAP because it is the more secure of the two protocols.
PAP

To understand how PAP works, imagine a network topology where a remote office router (Cisco 805 router) is connected to a corporate office router (such as a 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.

### Table C-2 PAP and CHAP Comparison

<table>
<thead>
<tr>
<th>Authentication Protocol</th>
<th>Controls Authentication Attempt(s)</th>
<th>Handshake Method</th>
<th>Password</th>
<th>Protection from Playback or Repeated Attacks?</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHAP</td>
<td>Corporate office router (local node)</td>
<td>Three-way. Corporate office router sends challenge to remote office router. Remote office router responds. Corporate office router accepts or rejects authentication.</td>
<td>Uses variable, unique, and unpredictable challenge value.</td>
<td>Yes, through the challenge variable and repeated challenges after the link has been established.</td>
</tr>
</tbody>
</table>
CHAP

To understand how CHAP works, imagine a network topology where a remote office router (Cisco 805 router) is connected to a corporate office router (such as a 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 provides protection 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.

Dialer Profiles

You can use dialer profiles to configure the router physical (serial) interface separately from the logical configuration required for a call. You can also configure the router to allow the logical and physical configurations to be dynamically bound together on a per-call basis. All calls going to or from a destination subnetwork use the same dialer profile.

A dialer profile consists of the following elements:

- A dialer interface (a logical entity) configuration with one or more dial strings, each used to reach a specific destination subnetwork.
- A dialer map class defining all the characteristics for any call to the specified dial string (telephone number). This element is optional; it is typically used to specify ISDN speeds. Because the Cisco 805 router has only a serial interface, the sample networks specify the call characteristics with the dialer interface configuration rather than defining a dialer map class.
- A dialer pool of physical interfaces to be used by the dialer interface. The physical interfaces in a dialer pool are ordered according to priority.
Dialer Profiles

Dialer Interface

A **dialer interface** is a WAN interface on the router that is not connected to a remote device all the time but which dials the remote device whenever a connection is required. Configuring an interface on a Cisco router to dial a specific remote device at specific times requires configuring dialer profiles.

A dialer interface configuration is a group of settings the router uses to connect to a remote network. One dialer interface can use multiple dial strings (telephone numbers). Each dial string is associated with its own dialer map class. The dialer map class defines all the characteristics for any call to the specified dial string. For example, the dialer map class for one destination might specify the amount of idle time as 3 seconds before calls are disconnected, and the map class for a different destination might specify 10 seconds.

Dialer Pool

Each dialer interface uses one group of physical interfaces called a **dialer pool**. One physical interface can belong to multiple dialer pools.

When you use dialer profiles to configure dial-on-demand routing (DDR), the physical interface is configured only for encapsulation and the dialer pools to which the interface belongs. All other characteristics used for making calls are defined in the dialer map.
Connecting Cisco Equipment to Other Vendor Equipment

This appendix contains information that you will need if you connect your Cisco 805 router to an Ascend router.

When configuring your router, perform the following steps in addition to those discussed in Chapter 3, “Configuring Remote Office to Corporate Office Networks” and in Chapter 4, “Configuring Small Office to ISP Networks.”

**Step 1** Set up a username-based authentication system:

```
username name password <password>
```

You need to enter this command twice: to specify the Ascend router username and password and to specify the Cisco router username and password. For example:

```
router (config)# username max200 password letmein
router (config)# username c805 password letmein
```

**Step 2** When setting up a dialer map using the following command, make sure that you specify the Ascend router name for authentication:

```
dialer map ip next-hop-address name hostname speed 56 dial-string
```

For example:

```
router (config-if)# dialer map 192.168.214.1 name max200 speed 56 5551234
```
Step 3  Make sure to set up either PAP or CHAP by entering one of the following comments, respectively:

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

router (config-if)# ppp authentication chap callin
```
Recovering a Lost Enable Password

This appendix describes how to recover a password that you configured with the `enable` command (enable password).

**Note** You can recover a lost enable password, but not a password that you configured with the `enable secret` command (enable secret password). This password is encrypted and must be replaced with a new enable secret password. See the “Hot Tips” section on Cisco Connection Online (CCO) for information on replacing enable secret passwords.

Follow these steps to recover a lost enable password:

**Step 1** Connect an ASCII terminal or a PC running a terminal emulation program to the Console port. For more information, see the *Cisco 805 Router Hardware Installation Guide*.

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

**Step 3** Reboot the router.

**Step 4** From user EXEC mode, display the existing configuration register value:

```
Router> show version
```

**Step 5** Record the setting of the configuration register. The setting is usually 0x2102 or 0x102.

**Step 6** 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` global configuration command.

**Step 7** Do one of the following:

- If break is enabled, go to Step 8.
- If break is disabled, turn the router to STANDBY, wait 5 seconds, and turn it to ON again. Before the terminal displays `Boot....`, press **Escape** or **Control-C**. The terminal displays the ROM monitor prompt (`boot #`). Go to Step 9.

Note Some terminal keyboards have a key labeled **Break**. If your keyboard does not have a Break key, refer to the documentation that came with the terminal for instructions on how to send a break.

**Step 8** Send a break. The terminal displays the following prompt:

```
boot#
```

**Step 9** Reset the configuration register:

```
boot# set ios-conf=142
```

**Step 10** Initialize the router:

```
boot# boot [flash]
```

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 11** Enter `no` in response to the prompts until the following message is displayed:

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

**Step 12** Press **Return**. The following prompt appears:

```
router>
```

---
Step 13  Enter privileged EXEC mode:
        router> enable

        The prompt changes to the privileged EXEC prompt:
        router#

Step 14  Display the enable password in the configuration file:
        router# show startup-config

Step 15  Enter configuration mode:
        router# configure terminal

Step 16  Reset the configuration register:
        router# config-register value

        Specify the value that you recorded in Step 5 (usually 0x2102 or 0x102).

Step 17  Press Ctrl-Z to exit configuration mode.

Note    To return to the configuration being used before recovering the lost enable password, 
do not save the configuration changes before rebooting the router.

Step 18  Reboot the router, and enter the recovered password.
Common Port Assignments

Table F-1 lists currently assigned Transmission Control Protocol (TCP) port numbers. To the extent possible, the User Datagram Protocol (UDP) uses the same numbers.

<table>
<thead>
<tr>
<th>Port</th>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>–</td>
<td>Reserved</td>
</tr>
<tr>
<td>1–4</td>
<td>–</td>
<td>Unassigned</td>
</tr>
<tr>
<td>5</td>
<td>RJE</td>
<td>Remote job entry</td>
</tr>
<tr>
<td>7</td>
<td>ECHO</td>
<td>Echo</td>
</tr>
<tr>
<td>9</td>
<td>DISCARD</td>
<td>Discard</td>
</tr>
<tr>
<td>11</td>
<td>USERS</td>
<td>Active users</td>
</tr>
<tr>
<td>13</td>
<td>DAYTIME</td>
<td>Daytime</td>
</tr>
<tr>
<td>15</td>
<td>NETSTAT</td>
<td>Who is up or NETSTAT</td>
</tr>
<tr>
<td>17</td>
<td>QUOTE</td>
<td>Quote of the day</td>
</tr>
<tr>
<td>19</td>
<td>CHARGEN</td>
<td>Character generator</td>
</tr>
<tr>
<td>20</td>
<td>FTP-DATA</td>
<td>File Transfer Protocol (data)</td>
</tr>
<tr>
<td>21</td>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>23</td>
<td>TELNET</td>
<td>Terminal connection</td>
</tr>
<tr>
<td>25</td>
<td>SMTP</td>
<td>Simple Mail Transport Protocol</td>
</tr>
<tr>
<td>37</td>
<td>TIME</td>
<td>Time</td>
</tr>
<tr>
<td>39</td>
<td>RLP</td>
<td>Resource Location Protocol</td>
</tr>
<tr>
<td>Port</td>
<td>Keyword</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>42</td>
<td>NAMESERVER</td>
<td>Host name server</td>
</tr>
<tr>
<td>43</td>
<td>NICNAME</td>
<td>Who is</td>
</tr>
<tr>
<td>49</td>
<td>LOGIN</td>
<td>Login Host Protocol</td>
</tr>
<tr>
<td>53</td>
<td>DOMAIN</td>
<td>Domain name server</td>
</tr>
<tr>
<td>67</td>
<td>BOOTPS</td>
<td>Bootstrap Protocol server</td>
</tr>
<tr>
<td>68</td>
<td>BOOTPC</td>
<td>Bootstrap Protocol client</td>
</tr>
<tr>
<td>69</td>
<td>TFTP</td>
<td>Trivial File Transfer Protocol</td>
</tr>
<tr>
<td>75</td>
<td>–</td>
<td>Any private dial-out service</td>
</tr>
<tr>
<td>77</td>
<td>–</td>
<td>Any private RJE service</td>
</tr>
<tr>
<td>79</td>
<td>FINGER</td>
<td>Finger</td>
</tr>
<tr>
<td>95</td>
<td>SUPDUP</td>
<td>SUPDUP Protocol</td>
</tr>
<tr>
<td>101</td>
<td>HOST NAME</td>
<td>NIC host name server</td>
</tr>
<tr>
<td>102</td>
<td>ISO-TSAP</td>
<td>ISO-TSAP&lt;sup&gt;1&lt;/sup&gt;</td>
</tr>
<tr>
<td>103</td>
<td>X400</td>
<td>X400</td>
</tr>
<tr>
<td>104</td>
<td>X400-SND</td>
<td>X400-SND</td>
</tr>
<tr>
<td>111</td>
<td>SUNRPC</td>
<td>SUN remote procedure call</td>
</tr>
<tr>
<td>113</td>
<td>AUTH</td>
<td>Authentication service</td>
</tr>
<tr>
<td>117</td>
<td>UUCP-PATH</td>
<td>UUCP&lt;sup&gt;2&lt;/sup&gt; path service</td>
</tr>
<tr>
<td>119</td>
<td>NNTP</td>
<td>Usenet Network News Transfer Protocol</td>
</tr>
<tr>
<td>123</td>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>126</td>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>137</td>
<td>NETBIOS-NS</td>
<td>NETBIOS name service</td>
</tr>
<tr>
<td>138</td>
<td>NETBIOS-DGM</td>
<td>NETBIOS datagram service</td>
</tr>
<tr>
<td>139</td>
<td>NETBIOS-SSN</td>
<td>NETBIOS session service</td>
</tr>
<tr>
<td>161</td>
<td>SNMP</td>
<td>Simple Network Management Protocol Q/R</td>
</tr>
<tr>
<td>162</td>
<td>SNMP-TRAP</td>
<td>Simple Network Management Protocol traps</td>
</tr>
<tr>
<td>Port</td>
<td>Keyword</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>512</td>
<td>rexec</td>
<td>UNIX rexec (Control)</td>
</tr>
<tr>
<td>513</td>
<td>TCP—rlogin</td>
<td>TCP—UNIX rlogin</td>
</tr>
<tr>
<td></td>
<td>UDP—rwho</td>
<td>UDP—UNIX broadcast name service</td>
</tr>
<tr>
<td>514</td>
<td>TCP—rsh</td>
<td>TCP—UNIX rsh and rep</td>
</tr>
<tr>
<td></td>
<td>UDP—syslog</td>
<td>UDP—UNIX system log</td>
</tr>
<tr>
<td>515</td>
<td>Printer</td>
<td>UNIX line printer remote spooling</td>
</tr>
<tr>
<td>520</td>
<td>RIP</td>
<td>Routing Information Protocol</td>
</tr>
<tr>
<td>525</td>
<td>Timed</td>
<td>Time server</td>
</tr>
</tbody>
</table>

1 TSAP=Transport Service Access Point
2 UUCP=UNIX-to-UNIX Copy Protocol
accessing ROM monitor  A-1
Ascend routers, configuration  D-1
asynchronous modem
  See dial-up line
authentication protocols
  CHAP  C-3, C-5
  PAP  C-3, C-4

bandwidth requirements, and WAN options  1-5
booting from TFTP server  A-9

Challenge Handshake Authentication Protocol
  See CHAP
  CHAP  C-3, C-5
Cisco IOS
  See IOS
CiscoView  1-10
CLI
  basic skills  2-1
  configuring router  3-1, 4-1, 5-13
  error messages  2-9
  help  2-6
  saving changes  2-10
  upgrading software  B-1
command-line interface
  See CLI
commands
  configure  2-4, 2-5
  configure terminal  2-8
  conventions  xiii
  copy running-config startup-config  2-10
  disable  2-4
  enable  2-4, 2-7, E-1
  enable secret  2-7
  end  2-5
  error messages  2-9
  exit  2-5
  help, accessing  2-6
  how to use  2-8
  interface  2-5
  line  2-6
  logout  2-4
  modes, understanding  2-3
  ROM monitor  A-6
  router  2-5
ConfigMaker software  1-9
configuration
  initial dialog  2-8
  IOS basic skills  2-1
  saving changes  2-10
configuration mode  2-7
configuration parameters, ROM monitor  A-3
configure command  2-4, 2-5
configure terminal command  2-8
configuring router
  from PC  2-2
  software options  4-1
  firewall  5-13
  overview  1-9
  remote office to corporate office networks  3-1
  conventions, command  xiii
  cost, and WAN options  1-5

DHCP
  relay  3-32, 5-8, 5-17
server 3-22, 5-7
dialer profiles 3-22, 4-8, C-5
dial-up line 3-22, 4-8
   activation 1-1, 1-2, 5-8
   controlling 5-15
   bandwidth 1-5
disable command 2-4
documentation set, Cisco IOS xv
Dynamic Host Configuration Protocol
   See DHCP

E

Easy IP (Phase 1) 1-7, 4-8, 5-2
Easy IP (Phase 2) 1-7
   configuring 5-6
   remote office to corporate office
dial-up, PPP 3-22
   Frame Relay 3-32
EIGRP 5-2, C-1, C-3
   enable command 2-4, 2-7
   enable secret command 2-7
   encapsulation, WAN 1-4, 1-6, 3-1, 4-1
   end command 2-5
Enhanced Interior Gateway Routing Protocol
   See EIGRP
error messages 2-9
examples 1-2
examples, network remote office to corporate office 3-1
   small office to ISP 4-1
exit command 2-5

F

Fast Step software

firewall 5-13

overview 1-9
remote office to corporate office networks 3-1
small office to ISP networks 4-1
features C-3
CHAP C-3, C-5
DHCP
   relay 5-8, 5-17
   server 5-7
Easy IP (Phase 1) 1-7, 4-8, 5-2
Easy IP (Phase 2)
   configuring 5-6
   overview 1-7
   remote office to corporate office, dial-up,
   PPP 3-22
   remote office to corporate office, Frame Relay 3-32
EIGRP C-1
firewall
   configuring 5-13
   overview 1-8
   small office to ISP, dial-up, PPP 4-8
   small office to ISP, Frame Relay 4-17
NAT overload 1-8, 4-17, 5-10
PAP C-3, C-4
RIP C-1, C-2
SNTP 5-18
Windows NT 5-14, 5-16

firewall
   configuring 5-13
   overview 1-8
   small office to ISP
dial-up, PPP 4-8
   Frame Relay 4-17

firmware
   See ROM monitor
Frame Relay 3-31, 4-16
   bandwidth 1-5
   partially meshed topology 3-31
   subinterfaces 3-32
Index 3

G

global configuration mode 2-7
glossary xiii

H

HDLC 1-6, 3-5
help
  CLI 2-6
  ROM monitor A-6
High-Level Data Link Control
  See HDLC
HyperTerm software 2-2

I

initial configuration dialog 2-8
interface command 2-5
IOS
  documentation set xv
  software 1-10, 3-1, 4-1
  basic skills 2-1
IP address
  assigning 5-6
  registered
    buying 4-3
    negotiating 5-2
  unregistered
    accessing Internet 4-17
    translating to registered 5-10
IP traffic 5-19
IPX traffic 5-21

L

LAN, components of 1-1
leased line 3-5, 3-10, 4-3
line command 2-6
logout command 2-4

M

messages, error 2-9
modes
  command, understanding 2-3
  global configuration 2-7
  ROM monitor A-2
  setup 2-8

N

NAT 1-7, 4-8, 5-2
NAT overload 1-8, 4-17, 5-10
Network Address Translation
  See NAT
Network Address Translation overload
  See NAT overload
network examples 1-2
  remote office to corporate office 3-1
  small office to ISP 4-1
network management 1-10

P

PAP C-3, C-4
parameters, ROM monitor A-3
Password Authentication Protocol
  See PAP
passwords
recovering lost enable E-1
ROM monitor A-2
router 2-7

PAT
See NAT overload
Point-to-Point Protocol
See PPP
Point-to-Point Protocol/Internet Protocol Control Protocol
See PPP/IPCP
Port Address Translation
See NAT overload
port assignments F-1

PPP
overview 1-6
remote office to corporate office
dial-up line 3-22
leased line 3-10
small office to ISP
dial-up 4-8
leased line 4-3
PPP/IPCP 1-7, 4-8, 5-2
ProComm software 2-2
protocols
routed 1-6
routing 1-6, C-1
protocols, authentication
CHAP C-3, C-5
PAP C-3, C-4

R
remote-office-to-corporate-office networks 1-2, 3-1, 4-1
before configuring 3-3
dial-up line, PPP 3-22
Frame Relay 3-31
leased line, HDLC 3-5
leased line, PPP

remote office to corporate office, leased line 3-10
X.25 3-15
RIP C-1, C-2
ROM monitor A-1
routed protocols 1-6
router command 2-5
routers from other vendors, configuration D-1
Routing Information Protocol
See RIP
routing protocols 1-6, C-1

S
sample networks 1-2
remote office to corporate office 3-1
small office to ISP 4-1
saving configuration changes 2-10
security
CHAP C-3, C-5
PAP C-3, C-4
router 2-7
small-office-to-ISP network 5-22
settings, VT-100 2-2
setup mode 2-8
Simple Network Time Protocol
See SNTP
small-office-to-ISP networks 1-2, 4-1
before configuring 4-2
dial-up line, PPP 4-8
Frame Relay 4-16
leased line, PPP 4-3
restricting access 5-22
SNTP 5-18
software, upgrading B-1
from CLI B-1
from ROM monitor B-3
static routes
IP
overview 1-6
remote office to corporate office, dial-up, PPP 3-22
small office to ISP, dial-up, PPP 4-8
small office to ISP, Frame Relay 4-16
small office to ISP, leased line, PPP 4-3
IPX 1-6, 3-22
subinterfaces 3-32
system software
See ROM monitor

T

terminal emulation software 2-2
Terminal software 2-2
terms, defined xiii
TFTP server
boots from A-9
downloading software from B-2, B-5
traffic
IP 5-19
IPX 5-21
Trivial File Transfer Protocol server
See TFTP server

U

upgrading software B-1
from CLI B-1
from ROM monitor B-3

V

VersaTerm software 2-2

W

WAN encapsulation
Frame Relay 3-31, 4-16
HDLC 3-5
overview 1-4, 1-6
PPP
remote office to corporate office, dial-up 3-22
remote office to corporate office, leased line 3-10
small office to ISP, dial-up 4-8
small office to ISP, leased line 4-3
remote office to corporate office 3-1
small office to ISP 4-1
X.25 3-15

WAN options
dial-up line 3-22, 4-8
Frame Relay 3-31, 4-16
leased line 3-5, 3-10, 4-3
overview 1-4, 1-5
remote office to corporate office 3-1
small office to ISP 4-1
X.25 3-15

WAN, components of 1-1
Windows NT 5-14, 5-16

X

X.25 3-15