Cisco Reader Comment Card

General Information

1 Years of networking experience: _____ Years of experience with Cisco products: _____

2 I have these network types: ☐ LAN ☐ Backbone ☐ WAN
☐ Other: _____

3 I have these Cisco products: ☐ Switches ☐ Routers
☐ Other (specify models): _____

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

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

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

7 I prefer this access method: _____

8 I use the following three product features the most:

Document Information

Document Title: Cisco 1700 Series Router Software Configuration Guide

Part Number: 78-5407-03

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

_____ The document is written at my technical level of understanding.
_____ The information is accurate.
_____ The document is complete.
_____ The information I wanted was easy to find.
_____ The information is well organized.
_____ The information I found was useful to my job.

Please comment on our lowest scores:

Mailing Information

Company Name Date

Contact Name Job Title

Mailing Address

City State/Province ZIP/Postal Code

Country Phone ( ) Extension

Fax ( ) E-mail

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

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

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 4631 SAN JOSE CA

POSTAGE WILL BE PAID BY ADDRESSEE

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

Cisco 1700 Series Router Software Configuration Guide

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

Customer Order Number: DOC-785407=
Text Part Number: 78-5407-03

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

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

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

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

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

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

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

Cisco 1700 Series Router Software Configuration Guide
Copyright © 2002, Cisco Systems, Inc.
All rights reserved.

CONTENTS

CHAPTER 7

Preface

This preface describes the objectives, audience, organization, and conventions of the *Cisco 1700 Series Router Software Configuration Guide*. It also provides information about additional documentation and about how to obtain technical assistance.

Objectives

This software configuration guide explains how to configure Cisco 1700 routers. It does not cover every feature, but it does describe, in detail, the tasks most commonly required for configuring the router.

This guide also references detailed features described in the Cisco IOS configuration guides and command references. Refer to those other books for additional information.

Audience

This guide is intended both for network administrators who have no or little experience configuring routers and for network administrators who have extensive experience. This guide is useful for both the following situations:

- You have a router that is already configured, and you want to configure additional features, using the command-line interface (CLI).
- You want to configure the router by using only the CLI.

Organization

This document contains the following chapters and appendixes:

- Chapter 1, "Introduction to Router Configuration"—Describes what you need to know about the Cisco IOS software (the software that runs the router) before you begin to configure the router.
- Chapter 2, "Configuring Security Features"—Describes how to configure security features on Cisco routers, including IP Security (IPSec), firewalls, and virtual private dial-up networks (VPDNs).
- Chapter 3, "Miscellaneous Features"—Provides procedures for configuring miscellaneous features of the Cisco 1700 Series routers: Dynamic Host Configuration Protocol (DHCP) and Network Address Translation (NAT).
- Chapter 4, "Configuring Routing Among VLANs with IEEE 802.1Q Encapsulation"—Describes the required and optional tasks for configuring routing between VLANs with IEEE 802.1Q encapsulation.
- Chapter 5, "Configuring ISDN"—Describes how to configure a Cisco router to dial into a central-site router over an Integrated Services Digital Network (ISDN) line.
- Chapter 6, "Configuring a Leased Line"—Describes how to configure a Cisco router for Internet Protocol (IP) and Internetwork Packet Exchange (IPX) over a private synchronous serial line.
- Chapter 7, "Configuring Frame Relay"—Describes how to configure a Cisco router to connect to a central-site router over a Frame Relay line.
- Chapter 8, "Configuring Asynchronous Connections"—Describes how to configure a Cisco router to dial into a central-site router over a standard telephone line.
- Chapter 9, "Configuring X.25"—Describes how to configure a Cisco router to connect to a central-site router over an X.25 line.
- Appendix A, "Networking Concepts"—Describes concepts that can help you in designing your network and configuring your router according to the examples in this guide.
- Appendix B, "ROM Monitor"—Describes the functions and commands of the router ROM monitor (also called the *bootstrap program*), the firmware that runs when the router is powered up or reset.

Conventions

This document uses the following conventions:

- The caret character (^) represents the Control key.

  For example, the key combinations ^D and Ctrl-D mean the same thing: Hold down the Control key while you press the D key. Although keys are indicated in capital letters, they are not case sensitive.

Command descriptions use these conventions:

- Commands and keywords in **boldface** font.
- Variables for which you supply values are in *italic* font.

Examples use these conventions:

- Examples that contain system prompts denote interactive sessions, indicating that you enter commands at the prompt. The system prompt indicates the current command mode. For example, the following prompt indicates global configuration mode:

  ```
  Router(config)#
  ```

- Terminal sessions and information that the system displays are in `screen` font.
- Information that you enter is in **`boldface screen`** font.
- Nonprinting characters, such as passwords, are in angle brackets (< >).

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

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

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

Related Documentation

The following publications provide related information about this product:

- Cisco IOS command references and configuration guides for Cisco IOS Release 12.2 provide complete information about all Cisco IOS CLI commands and how to use them, as well as information on designing and configuring LANs and WANs.
- The Quick Start Guide that comes with your router has instructions for quickly cabling and powering up the router.
- The Hardware Installation Guide for your router, which is available online, describes router features, tells how to install and cable the router, and tells how to troubleshoot common problems you may have with it.

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

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

http://www.cisco.com

Translated documentation is available at the following URL:

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

Documentation CD-ROM

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

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Feedback** at the top of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

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

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

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

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

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

http://www.cisco.com/register/

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

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

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

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

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

CHAPTER 1

Introduction to Router Configuration

If you understand Cisco IOS software (the software that runs your router) and you are experienced in configuring network devices, you can use the Cisco IOS command-line interface (CLI) to configure your router. This guide will help you use Cisco IOS software to configure your router. This chapter tells you what you need to know before you begin configuring your router with Cisco IOS software.

This chapter contains the following sections:

- Configuring the Router from a PC
- Understanding Command Modes
- Getting Help
- Enable Secret and Enable Passwords
- Entering Configuration Mode
- Using Commands
- Saving Configuration Changes
- Using Debug Commands
- Where to Go Next

Understanding these concepts saves you time when you are configuring your router. If you have never used the Cisco IOS software or if you need a refresher, read this chapter before you proceed to the next chapter.

If you are already familiar with the Cisco IOS software, you can proceed to the configuration chapter that is appropriate for your network.

Configuring the Router from a PC

If you are configuring your router from a PC (not a dumb terminal), you need a type of communications software called *terminal emulation* software. The PC uses this software to send commands to your router. Table 1-1 lists some common names for this software, based on the type of PC you are using.

Table 1-1 Terminal Emulation Software

PC Operating System	Software
Windows 95, Windows NT	HyperTerminal (included with Windows software)
Windows 3.1	Terminal (included with Windows software)
Macintosh	ProComm, VersaTerm (supplied separately)

You can use the terminal emulation 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 settings, so that your PC can communicate with your router:

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

You can now configure your router by using your PC.

Understanding Command Modes

This section describes the Cisco IOS command mode structure. Each command mode supports specific Cisco IOS commands. For example, the **interface** *type_number* command is used only when in global configuration mode.

You use the following Cisco IOS command modes when configuring the scenarios described in this document:

- User EXEC
- Privileged EXEC
- Global configuration
- Interface configuration
- Router configuration
- Line configuration

Note Throughout the examples in this guide, there are steps for verifying your router configuration by using different Cisco IOS commands. If you plan to use these verification steps, you must understand how to change from one command mode to another; for this information, see Table 1-2.

Table 1-2 lists the command modes that are used in this guide, tells how to access each mode, identifies the prompt you see in each mode, and tells how to exit each mode. The examples in the table use the host name *Router*.

Table 1-2 Command Modes Summary

Mode	Access Method	Prompt	Exit Method	About This Mode[1]
User EXEC	Begin a session with your router.	`Router>`	Enter the **logout** command.	Use this mode to • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	Enter the **enable** command while in user EXEC mode.	`Router#`	• To exit to user EXEC mode, enter the **disable** command. • To enter global configuration mode, enter the **configure** command.	Use this mode to • Configure your router operating parameters. • Perform the verification steps shown in this guide. You should configure your router with an enable password to prevent anyone from making unauthorized changes to the router configuration.

Table 1-2 Command Modes Summary (continued)

Mode	Access Method	Prompt	Exit Method	About This Mode[1]
Global configuration	Enter the **configure** command while in 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.
Interface configuration	Enter the **interface** command (with a specific interface) while in the global configuration mode.	`Router(config-if)#`	• To exit to global configuration mode, enter the **end** command. • To exit to privileged EXEC mode, enter the **exit** 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 various LAN interfaces of your router, including the following: • 10BASE-T Ethernet interface. • 10/100BASE-T Fast Ethernet interface.

Table 1-2 Command Modes Summary (continued)

Mode	Access Method	Prompt	Exit Method	About This Mode[1]
Router configuration	Enter your router command, followed by the appropriate keyword, while in global configuration mode.	`Router(config-router)#`	• To exit to global configuration mode, enter the **end** command. • To exit to privileged EXEC mode, enter the **exit** command, or press **Ctrl-Z**.	Use this mode to configure an IP routing protocol.
Line configuration	Specify a line with the **line vty** command while in the global configuration mode.	`Router(config-line)#`	• To exit to global configuration mode, enter the **exit** command. • To enter privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.	Use this mode to configure parameters for the terminal line.

1. You can see a comprehensive list of the commands available for any mode by entering a question mark (?) at the prompt.

Getting Help

Here are some ways to get help while in any command mode:

- Enter a question mark to list the commands that are available in the current mode. You can restrict the list to all commands starting with a specific letter by entering that letter, followed by a question mark (no space):

```
Router (config-if)# s?
  shutdown
  snapshot
  snmp
  standby
```

- Enter a command, a space, and a question mark to see a list of the available keywords (and a short definition of the keywords) that can be used with the command:

```
Router (config-if)# snapshot ?
  client Enable client control of Snapshot routing
  server Send routing updates out this link when updates are
received
```

- Enter a command, a keyword, a space, and a question mark to see a list of the range of values (and a short definition of the values) that you can enter with the command:

```
Router (config-if)# snapshot client ?
  <5-1000> duration, in minutes, of each active period
```

- Enter a few known characters to have the router complete the command. In this example, the command is **show hosts**:

```
Router> sh ho
Default domain is not set
Name/address lookup uses domain service
Name servers are 255.255.255.25
```

- To redisplay a command that you previously entered, press the **Up** arrow key. You can continue to press the **Up** arrow key for more commands. The commands are displayed in reverse order from that in which they were entered.

Enable Secret and Enable Passwords

Because many privileged EXEC commands are used to set operating parameters, you should password-protect these commands to prevent unauthorized use.

You 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 the "Troubleshooting" chapter in the *Hardware Installation Guide* that came with your router.

Entering Configuration Mode

To make any configuration changes to your router, you must be in configuration mode. This section describes how to enter configuration mode while using a terminal or PC that is connected to your router CONSOLE port.

To enter 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 If you have configured your router with an enable password, enter the **enable** command; then enter the enable password when you are prompted for it. The enable password is not displayed on the screen when you enter it.

This example shows how to enter enable mode on a Cisco router:

```
Router> enable
Password: <enable_password>
Router#
```

Enable mode is indicated by the pound sign (#) in the prompt.

Step 3 Enter the **configure terminal** command to enter 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 CLI.

Abbreviating Commands

You have to enter only enough characters for the router to recognize the command as unique. This example show how to enter the **show configuration** command:

```
Router# show conf
Using 385 out of 7506 bytes
!
version 12.2
no service udp-small-servers
no service tcp-small-servers
.
.
.
```

Command-Line Error Messages

Table 1-3 lists some error messages that you might encounter while using the CLI to configure your router.

Table 1-3 Common CLI Error Messages

Error Message	Meaning	How to Get Help
`% Ambiguous command: "show con"`	You did not enter enough characters for your router to recognize the command.	Reenter the command, followed by a question mark (?), with no space between the command and the question mark. The possible keywords that you can use with the command are displayed.
`% Incomplete command.`	You did not enter all of the keywords or values required by this command.	Reenter the command, followed by a question mark (?), with no space between the command and the question mark. The possible keywords that you can enter with the command are displayed.
`% Invalid input detected at '^' marker.`	You entered the command incorrectly. The error occurred where the caret mark (^) appears.	Enter a question mark (?). All the commands that are available in this command mode are displayed.

Undoing Commands

If you want to disable a feature or undo a command that you entered, you can enter the keyword **no** before most commands; for example, **no ip routing**.

Saving Configuration Changes

You need to enter the **copy running-config startup-config** command to save your configuration changes to nonvolatile random-access memory (NVRAM) so that they are not lost if there is a system reload or power outage. The following example shows how to use this command to save your changes:

```
Router# copy running-config startup-config
```

```
Building configuration...
```

Saving the configuration to NVRAM might require a minute or two. After the configuration has been saved, the following appears:

```
[OK]
Router#
```

Using Debug Commands

Debug command are provided for most of the configurations in this document. You can use the debug commands to troubleshoot any configuration problems that you might be having on your network. Debug commands provide extensive, informative displays to help you interpret problems.

Table 1-4 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. Debugging during these periods decreases the likelihood that the debug command processing overhead will affect network users.

Table 1-4 Important Information About Debug Commands

What	Information
Additional documentation	You can find additional information and documentation about the debug commands in the *Debug Command Reference* document on the Cisco IOS software documentation CD-ROM that came with your router. If you are not sure where to find this document on the CD-ROM, use the Search function in the Verity Mosaic browser that comes with the CD-ROM.
Disabling debugging	To turn off debugging, enter the **undebug all** command.
Telnet sessions	To use debug commands during a Telnet session with your router, you must first enter the **terminal monitor** command.

Where to Go Next

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

Keep in mind the following tips:

- 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**.
- You need to save your configuration changes to NVRAM so that they are not lost if there is a system reload or power outage.

CHAPTER 2

Configuring Security Features

This chapter presents basic configuration procedures for security features in the Cisco 1700 series routers. For a full description of these features and their configurations, please refer to the Cisco IOS command references and configuration guides for Cisco IOS Release 12.2.

This chapter contains the following sections:

- Configuring IP Security
- Configuring a Virtual Private Dial-Up Network
- Configuring Firewalls

Configuring IP Security

IP Security (IPSec) is a framework of open standards for ensuring secure private communications over IP networks. Based on standards developed by the Internet Engineering Task Force (IETF), IPSec ensures confidentiality, integrity, and authenticity of data communications across a public IP network. Cisco's realization of IPSec implements the Data Encryption Standard (DES) and triple DES (3DES).

Refer to the *Cisco IOS Security Configuration Guide, Release 12.2*, for more detailed information on IPSec.

Perform the following tasks to configure IPSec. Start in global configuration mode.

	Command	Task
Step 1	**crypto isakmp policy 10**	Define an Internet Key Exchange (IKE) policy, and assign the policy a priority. This command places the router in IKE policy configuration mode.
Step 2	**hash** *algorithm*	Specify the hash algorithm for the policy.
Step 3	**encryption** *encryption*	Specify the encryption for the policy.
Step 4	**authentication pre-share**	Specify pre-share key as the authentication method.
Step 5	**exit**	Exit IKE policy configuration mode.
Step 6	**crypto isakmp key** *name* **address** *ip-address*	Configure a pre-share key and static IP address for each VPN client.
Step 7	**crypto ipsec transform-set** *name* **esp-***encryption* **esp-***hash algorithm***-hmac**	Define a combination of security associations to occur during IPSec negotiations.
Step 8	**crypto mib ipsec flowmib history tunnel size** *size*	Set the size of the tunnel history table.
Step 9	**crypto mib ipsec flowmib history failure size** *size*	Set the size of the failure history table.
Step 10	**crypto map** *name* **local-address Ethernet 0**	Specify and name an identifying interface to be used by the crypto map for IPSec traffic
Step 11	**crypto map** *name seq-num* **ipsec-isakmp**	Create a crypto map entry in IPSec Internet Security Association and Key Management Protocol (ISAKMP) mode, and enter crypto map configuration mode.
Step 12	**set peer** *ip-address*	Identify the remote IPSec peer.
Step 13	**set transform-set** *name*	Specify the transform set to be used.
Step 14	**set pfs [group1|group2]**	Specify use of the perfect forward secrecy (pfs) option in IPSec. The variation **group1** is the default.
Step 15	**match address** *access-list-id*	Specify an extended access list for the crypto map entry.
Step 16	**exit**	Exit crypto map configuration mode.

Disabling Hardware Encryption

If your Cisco 1700 series router is equipped with an optional Virtual Private Network (VPN) module, it provides hardware 3DES encryption by default. If you wish, you can disable the VPN module and use Cisco IOS software encryption/decryption instead.

The command that disables the VPN module is as follows:

no crypto engine accelerator

The command is executed in configuration mode. The following is an example of its use:

```
Router(config)#no crypto engine accelerator
Warning! all current connections will be torn down.
Do you want to continue? [yes/no]: yes
.
Crypto accelerator in slot 0 disabled
.
switching to IPsec crypto engine
```

After this command is executed, the following procedure must be performed to bring up all encryption tunnels appropriately.

Step 1 On all the routers involved, shut down the interfaces that have crypto maps.

Step 2 Enter the following commands on each router.

Command	Task
clear crypto sa	Clear the security associations applied to the router.
clear crypto isakmp	Clear the active IKE connections to the router.
show crypto engine connections active	List the active connections. In this scenario, this command verifies that no connections are active.

You may need to repeat these commands until no connections are listed.

Step 3 Bring up the interfaces on all the routers that were shut down in Step 1.

To reenable the VPN module, use the following command:

crypto engine accelerator

For example:

```
Router(config)#crypto engine accelerator
Warning! all current connections will be torn down.
Do you want to continue? [yes|no]:yes
.
switching to crypto accelerator.
```

The following is a useful command that shows statistical information about the VPN module:

show crypto engine accelerator statistic

For example:

```
Router#show crypto engine accelerator statistic
C1700_EM:
  ds: 0x81784BA4 idb:0x81780560
  Statistics for Virtual Private Network (VPN) Module:
     0 packets in        0 packets out
     0 paks/sec in       0 paks/sec out
     0 Kbits/sec in      0 Kbits/sec out
  rx_no_endp: 0 rx_hi_discards: 0 fw_failure: 0
  invalid_sa: 0 invalid_flow: 0 cgx_errors 0
  fw_qs_filled: 0 fw_resource_lock:0 lotx_full_err: 0
  null_ip_error: 0 pad_size_error: 0 out_bound_dh_acc: 0
  esp_auth_fail: 0 ah_auth_failure: 0 crypto_pad_error: 0
  ah_prot_absent: 0 ah_seq_failure: 0 ah_spi_failure: 0
  esp_prot_absent:0 esp_seq_fail: 0 esp_spi_failure: 0
  obound_sa_acc: 0 invalid_sa: 0 out_bound_sa_flow: 0
  invalid_dh: 0 bad_keygroup: 0 out_of_memory: 0
  no_sh_secret: 0 no_skeys: 0 invalid_cmd: 0
  dsp_coproc_err: 0 comp_unsupported:0 pak_too_big: 0
  pak_mp_length_spec_fault: 0
  tx_lo_queue_size_max 0 cmd_unimplemented: 0
  159405 seconds since last clear of counters
  Interrupts: Notify = 0, Reflected = 0, Spurious = 0
  cgx_cmd_pending:0 packet_loop_max: 0 packet_loop_limit: 512
```

The **show crypto engine accelerator statistic** command can also be used as follows to verify that the VPN module is disabled.

For example:

```
Router#show crypto engine accelerator statistic
There is no crypto accelerator.
```

Configuring a Virtual Private Dial-Up Network

Complete the following tasks to configure a virtual private dial-up network (VPDN). Start in global configuration mode.

	Command	Task
Step 1	**vpdn enable**	Enable VPDN.
Step 2	**no vpdn logging**	Disable VPDN logging.
Step 3	**vpdn-group** *tag*	Configure a VPDN group.
Step 4	**request-dialin**	Specify the dialing direction.
Step 5	**protocol pppoe**	Specify the tunneling protocol as Point-to-Point Protocol over Ethernet (PPPoE).
Step 6	**end**	Exit router configuration mode.

Configuring Firewalls

Basic traffic filtering is limited to configured access list implementations that examine packets at the network layer or, at most, the transport layer, permitting or denying the passage of each packet through the firewall. However, the use of inspection rules in Context-based Access Control (CBAC) allows the creation and use of dynamic temporary access lists. These dynamic lists allow temporary openings in the configured access lists at firewall interfaces. These openings are created when traffic for a specified user session exits the internal network through the firewall. The openings allow returning traffic for the specified session (that would normally be blocked) back through the firewall.

Refer to the *Cisco IOS Security Configuration Guide, Release 12.2*, for more detailed information on traffic filtering and firewalls.

Access Lists

Access lists are configured as standard or extended. A standard access list either permits or denies passage of packets from a designated source. An extended access list allows designation of both the destination and the source, and it allows designation of individual protocols to be permitted or denied passage. An access list is a series of commands with a common tag to bind them together. The tag is either a number or a name.

Standard numbered access list commands take the following form:

access-list {1-99} {permit | deny} *source-addr [source-mask]*

Extended numbered access list commands take the following form:

access-list {100-199} {permit | deny} *protocol source-addr [source-mask] destination-addr [destination-mask]*

Named access list commands take the form:

ip access-list {standard | extended} *name*

A standard named access list command must be followed by subcommands in this form:

deny *{source | source-wildcard* **| any***}*

An extended named access list command must be followed by a subcommand in this form:

{permit | deny} *protocol {source-addr[source-mask]* **| any***} {destination-addr [destination-mask]* **| any**}

A sequence of access list commands bound together with a common name or number is referred to as an *access group*. An access group is enabled for an interface during interface configuration with the command

ip access-group *number|name* **[in | out]**

where **in | out** refers to the direction of travel of the packets being filtered.

When a sequence of access list commands is used, three things must be kept in mind:

- The order of commands in the sequence is important. A packet will be operated on by the first command. If there is no match (that is, if neither a permit nor a deny occurs), the next command operates on the packet, and so on.

- All matching parameters must be true before a command permits or denies access to a packet.
- There is an implicit “deny all” at the end of the sequence.

Configuration Examples

The following examples illustrate the configuration of standard numbered access lists and extended numbered access lists.

Configuring Standard Numbered Access Lists

In the following example, access list 2, a standard numbered access list, is defined to operate on the router, permitting or denying passage of packets associated with network 36.0.0.0. This network is a Class A network whose second octet specifies a subnet; that is, its subnet mask is 255.255.0.0. The third and fourth octets of a network 36.0.0.0 address specify a particular host. Using access list 2, the router would accept one address on subnet 48 and reject all others on that subnet. The last line of the list shows that the router would accept addresses on all other network 36.0.0.0 subnets.

```
access-list 2 permit 36.48.0.3
access-list 2 deny 36.48.0.0  0.0.255.255
access-list 2 permit 36.0.0.0  0.255.255.255
```

Note that all other accesses are implicitly denied.

The following commands tie the access group to a specific interface on the router and specify that incoming packets are to be permitted or denied passage:

```
interface ethernet 0
  ip access-group 2 in
```

Configuring Extended Numbered Access Lists

In the following example, access list 102, an extended numbered access list, is defined. The first command permits any incoming TCP messages with destination ports greater than 1023. The second command permits incoming TCP messages to the Simple Mail Transfer Protocol (SMTP) port of host 128.88.1.2. The third command permits incoming Internet Control Message Protocol (ICMP) messages for error feedback.

```
access-list 102 permit tcp 0.0.0.0 255.255.255.255 128.88.0.0 0.0.255.255 gt 1023
access-list 102 permit tcp 0.0.0.0 255.255.255.255 128.88.1.2 0.0.0.0 eq 25
access-list 102 permit icmp 0.0.0.0 255.255.255.255 128.88.0.0 255.255.255.255
```

The following commands tie the access group to a specific interface on the router and specify that incoming packets are to be permitted or denied passage:

```
interface ethernet 0
  ip access-group 102 in
```

Inspection Rules

Specify which protocols to examine by using the **ip inspect name** command. When inspection detects that the specified protocol is passing through the firewall, a dynamic access list is created to allow the passage of return traffic. The **timeout** parameter specifies the length of time the dynamic access list will remain active without return traffic passing through the router. When a timeout is reached, the dynamic access list is removed, and subsequent packets (possibly even valid ones) are not permitted.

For each protocol you want to inspect, enter a line in global configuration mode, using the following syntax:

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

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

CHAPTER 3

Miscellaneous Features

This chapter presents basic configuration procedures for miscellaneous features of the Cisco 1700 series routers. It contains the following sections:

- Configuring Dynamic Host Configuration Protocol
- Configuring Network Address Translation

Configuring Dynamic Host Configuration Protocol

The Dynamic Host Configuration Protocol (DHCP) is used to enable hosts (DHCP clients) on an IP network to obtain their configurations from a server (DHCP server). This reduces the work of administering an IP network. The most significant configuration option that the client receives from the server is its IP address.

Perform the following tasks to configure DHCP. Begin in global configuration mode.

	Command	Task
Step 1	**ip dhcp excluded-address** *low-ip-address high-ip-address*	Prevent DHCP from assigning one or more IP addresses to potential clients.
Step 2	**ip dhcp pool** *name*	Enter DHCP configuration mode, and create a pool of IP addresses that can be assigned to DHCP clients.
Step 3	**network** *address subnet-mask*	Specify a range of IP addresses that can be assigned to the DHCP clients.
Step 4	**default-router** *ip-address*	Specify the default router.
Step 5	**domain-name** *domain name*	Specify the domain name.
Step 6	**dns-server** *ip-address*	Specify the DNS server.
Step 7	**netbios-name-server** *ip-address*	Specify the NetBIOS name server.
Step 8	**netbios-node-type** *node-type*	Specify the NetBIOS node type.
Step 9	**lease** *days* **lease infinite**	Specify the duration of the lease.

Configuration Example

In the following example, three DHCP address pools are created: one in network 172.16.0.0, one in subnetwork 172.16.1.0, and one in subnetwork 172.16.2.0. Attributes from network 172.16.0.0, such as the domain name, Domain Name System (DNS) server, NetBIOS name server, and NetBIOS node type, are inherited in subnetworks 172.16.1.0 and 172.16.2.0. In each pool, clients are granted 30-day leases and all addresses in each subnetwork, except the excluded addresses, are available to the DHCP server for assigning to clients.

```
ip dhcp database ftp://user:password@172.16.4.253/router-dhcp
write-delay 120
ip dhcp excluded-address 172.16.1.100 172.16.1.103
ip dhcp excluded-address 172.16.2.100 172.16.2.103
!
ip dhcp pool 0
 network 172.16.0.0 /16
 domain-name cisco.com
```

```
 dns-server 172.16.1.102 172.16.2.102
 netbios-name-server 172.16.1.103 172.16.2.103
 netbios-node-type h-node
!
ip dhcp pool 1
 network 172.16.1.0 /24
 default-router 172.16.1.100 172.16.1.101
 lease 30
!
ip dhcp pool 2
 network 172.16.2.0 /24
 default-router 172.16.2.100 172.16.2.101
 lease 30
```

Configuring Network Address Translation

Network Address Translation (NAT) translates IP addresses within private "internal" networks to "legal" IP addresses for transport over public "external" networks (such as the Internet). Incoming traffic is translated back for delivery within the inside network. Thus, NAT allows an organization with unregistered "private" addresses to connect to the Internet by translating those addresses into globally registered IP addresses.

Interfaces are configured as "NAT inside" or "NAT outside." Once the interfaces are configured, the following steps can be performed to establish the NAT configuration within the router.

	Command	Task
Step 1	**ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}	Create a pool of global IP addresses for NAT.
Step 2	**access-list** *access-list-number* **permit** *source* [*source-wildcard*]	Define a standard access list permitting addresses that need translation.
Step 3	**ip nat inside source list** *access-list-number* **pool** *name* **[overload]**	Enable dynamic translation of addresses permitted by access list. **Overload** allows the use of one global address, from the pool, for many local addresses.
Step 4	**ip nat outside source static** *global-ip local-ip*	Enable static translation of a specified outside source address. This command is optional.

Configuration Example

In this example, we want NAT to allow certain devices on the inside to originate communication with devices on the outside by translating their internal addresses to valid outside addresses or a pool of addresses. The pool in this example is defined as the range of addresses from 172.16.10.1 through 172.16.10.63.

In order to accomplish this translation, we need to use dynamic NAT. With dynamic NAT, the translation table in the router is initially empty. The table is populated as traffic that needs to be translated passes through the router (in contrast with static NAT, in which a translation is statically configured and is placed in the translation table without the need for any traffic).

In this example, we can configure NAT to translate each inside device address to a unique valid outside address, or to translate each inside device address to the same valid outside address. The second method is known as *overloading*. An example of how to configure each method is given here.

To begin, configure the inside interface with an IP address and as a "NAT inside" interface.

```
interface inside interface
  ip address 10.10.10.1 255.255.255.0
  ip nat inside
```

Then configure the outside interface with an IP address and as a "NAT outside" interface.

```
interface outside interface
  ip address 172.16.10.64 255.255.255.0
  ip nat outside
```

To handle the case in which each inside address is translated to its own unique outside address, define a NAT pool named "no-overload" with a range of addresses from 172.16.10.0 to 172.16.10.63

```
ip nat pool no-overload 172.16.10.0 172.16.10.63 prefix 24
```

Define access list 7 to permit packets with source addresses ranging from 10.10.10.0 through 10.10.10.31 and from 10.10.20.0 through 10.10.20.31.

```
access-list 7 permit 10.10.10.0 0.0.0.31
access-list 7 permit 10.10.20.0 0.0.0.31
```

Then indicate that any packet received on the inside interface, as permitted by access list 7, will have its source address translated to an address from the NAT pool "no-overload."

```
ip nat inside source list 7 pool no-overload
```

Alternatively, when all inside addresses are translated to a single outside address, define a NAT pool named "ovrld," which has a range of a single IP address: 172.16.10.1.

```
ip nat pool ovrld 172.16.10.1 172.16.10.1 prefix 24
```

Then indicate that any packet received on the inside interface, as permitted by access list 7, will have its source address translated to the address from the NAT pool "ovrld." Translations will be overloaded, which will allow multiple inside devices to be translated to the same outside IP address.

```
ip nat inside source list 7 pool ovrld overload
```

The keyword **overload** used in this command allows NAT to translate multiple inside devices to the single address in the pool.

Another variation of this command is

```
ip nat inside source list 7 interface outside interface overload
```

which configures NAT to overload on the address that is assigned to the outside interface.

CHAPTER 4

Configuring Routing Among VLANs with IEEE 802.1Q Encapsulation

This chapter describes the required and optional tasks for configuring routing between virtual LANs (VLANs) with IEEE 802.1Q encapsulation. For complete descriptions of the VLAN commands used in this chapter, refer to the "Cisco IOS Switching Commands" chapter in the *Cisco IOS Switching Services Command Reference*. For descriptions of other commands that appear in this chapter, you can either use the command reference master index or search online.

The IEEE 802.1Q protocol is used to interconnect multiple switches and routers and to define VLAN topologies. IEEE 802.1Q support is available for Fast Ethernet interfaces.

This chapter contains the following sections:

- IEEE 802.1Q Encapsulation Configuration Task List
- Examples of IEEE 802.1Q Encapsulation Configuration
- VLAN Commands

IEEE 802.1Q Encapsulation Configuration Task List

You can configure routing among any number of VLANs in your network. This section provides procedures for configuring protocols supported with IEEE 802.1Q encapsulation. The basic process is the same, regardless of the protocol. The process involves the following:

- Enabling the protocol on the router
- Enabling the protocol on the interface
- Defining the encapsulation format as IEEE 802.1Q
- Customizing the protocol to meet the requirements for your environment

The configuration processes documented in this chapter include the following:

- Configuring IP Routing over IEEE 802.1Q
- Configuring IPX Routing over IEEE 802.1Q

Configuring IP Routing over IEEE 802.1Q

IP routing over IEEE 802.1Q extends IP routing capabilities to include support for routing IP frame types in VLAN configurations, using the IEEE 802.1Q encapsulation.

To route IP over IEEE 802.1Q between VLANs, you need to customize the subinterface to create the environment in which it will be used. Perform these tasks in the order in which they appear:

- Enabling IP Routing
- Defining the VLAN Encapsulation Format
- Assigning an IP Address to a Network Interface

Enabling IP Routing

IP routing is automatically enabled in the Cisco IOS software for routers. To reenable IP routing if it has been disabled, use the following command in global configuration mode:

ip routing

Once you have IP routing enabled on the router, you can customize the characteristics to suit your environment. If necessary, refer to the IP configuration chapters in the *Cisco IOS IP and IP Routing Configuration Guide* for guidelines on configuring IP.

Defining the VLAN Encapsulation Format

To define the encapsulation format as IEEE 802.1Q, use the following commands in interface configuration mode.

	Command	Task
Step 1	**interface fastethernet** *slot/port.subinterface-number* [1]	Specify the subinterface on which IEEE 802.1Q will be used.
Step 2	**encapsulation dot1q** *vlanid*	Define the encapsulation format as IEEE 802.1Q (**dot1q**) and specifies the VLAN identifier.

1. If the router supports only port numbers, and not slot numbers, the format for this command is **interface fastethernet** *port.subinterface-number*

Assigning an IP Address to a Network Interface

An interface can have one primary IP address. To assign a primary IP address and a network mask to a network interface, use the following command in interface configuration mode.

Command	Task
ip address *ip-address mask*	Set a primary IP address for an interface.

A mask identifies the bits that denote the network number in an IP address. When you use a mask to subnet a network, that mask is referred to as a *subnet mask*.

Configuring IPX Routing over IEEE 802.1Q

Internet Packet Exchange (IPX) Routing over IEEE 802.1Q VLANs extends Novell NetWare routing capabilities to include support for routing Novell Ethernet 802.3 encapsulation frame types in VLAN configurations. Users with Novell NetWare environments can configure Novell Ethernet 802.3 encapsulation frames to be routed, using IEEE 802.1Q encapsulation across VLAN boundaries.

To configure Cisco IOS software on a router with connected VLANs to exchange IPX Novell Ethernet 802.3 encapsulated frames, perform these tasks in the order in which they are appear:

- Enabling NetWare Routing
- Defining the VLAN Encapsulation Format
- Configuring NetWare on the Subinterface

Enabling NetWare Routing

To enable IPX routing on IEEE 802.1Q interfaces, use the following command in global configuration mode.

Command	Task
ipx routing *[node]*	Enable IPX routing globally.

Defining the VLAN Encapsulation Format

To define the encapsulation format as IEEE 802.1Q, use the following commands in interface configuration mode.

	Command	Task
Step 1	**interface fastethernet** *slot/port.subinterface-number*[1]	Specify the subinterface on which IEEE 802.1Q will be used.
Step 2	**encapsulation dot1q** *vlan-identifier*	Define the encapsulation format as IEEE 802.1Q and specify the VLAN identifier.

1. If the router supports only port numbers, and not slot numbers, the format for this command is **interface fastethernet** *port.subinterface-number*

Configuring NetWare on the Subinterface

After you enable NetWare globally and define the VLAN encapsulation format, you may need to enable the subinterface by specifying the NetWare network number. Use this command in interface configuration mode.

Command	Task
ipx network *network*	Specify the IPX network number.

Examples of IEEE 802.1Q Encapsulation Configuration

This section provides configuration examples for each of the protocols described in this chapter:

- Configuring IP Routing over IEEE 802.1Q
- Configuring IPX Routing over IEEE 802.1Q

Configuring IP Routing over IEEE 802.1Q

This configuration example shows IP being routed on VLAN 101:

```
!
ip routing
!
interface fastethernet 0.101
  encapsulation dot1q 101
  ip addr 10.0.0.11 255.0.0.0
!
```

Configuring IPX Routing over IEEE 802.1Q

This configuration example shows IPX being routed on VLAN 102:

```
!
ipx routing
!
interface fastethernet 0.102
  encapsulation dot1q 102
  ipx network 100
!
```

VLAN Commands

This section provides an alphabetical listing of all the VLAN commands that are new or specific to the Cisco router. All other commands used with this feature are documented in the Cisco IOS Release 12.1T command reference documents.

clear vlan statistics

To remove virtual LAN statistics from any statically configured or system-configured entries, use the **clear vlan statistics** privileged EXEC command:

clear vlan statistics

Syntax Description

This command has no arguments or keywords.

Default

No default behavior or values.

Command Mode

Privileged EXEC.

Example

The following example clears VLAN statistics:

```
clear vlan statistics
```

debug vlan packets

Use the **debug vlan packets** privileged EXEC command to display general information on virtual LAN (VLAN) packets that the router has received but that it is not configured to support:

debug vlan packets

The **no** form of this command disables debugging output:

no debug vlan packets

Syntax Description

This command has no arguments or keywords.

Command Mode

Privileged EXEC.

Usage Guidelines

The **debug vlan packets** command displays only packets with a VLAN identifier that the router is not configured to support. This command allows you to identify other VLAN traffic on the network. Virtual LAN packets that the router is configured to route or switch are counted and indicated when you use the **show vlans** command.

Example

The following is sample output from the **debug vlan packets** output:

```
Router# debug vlan packets
Virtual LAN packet information debugging is on
```

encapsulation dot1q

To enable IEEE 802.1Q encapsulation of traffic on a specified subinterface in virtual LANs, use the **encapsulation dot1q** command in subinterface configuration mode.

The command is as follows:

encapsulation dot1q *vlan-id*

Syntax Description

vlan-id	Virtual LAN identifier. The allowed range is from 1 to 4095 (in hexadecimal, from 0x1 to 0xfff).

Default

Disabled.

Command Mode

Subinterface configuration.

Usage Guidelines

IEEE 802.1Q encapsulation is configurable on Fast Ethernet interfaces.

Example

The following example encapsulates VLAN traffic, using the IEEE 802.1Q protocol for VLAN 100:

```
interface fastethernet 0.100
  encapsulation dot1q 100
```

show vlans

To view VLAN subinterfaces, use the **show vlans** privileged EXEC command:

show vlans

Syntax Description

This command has no arguments or keywords.

Command Mode

Privileged EXEC.

Example

The following is sample output from the **show vlans** command:

```
Router# show vlans

Virtual LAN ID:1 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interface: FastEthernet0

This is configured as native Vlan for the following interface(s):
FastEthernet0

   Protocols Configured: Address: Received: Transmitted:
```

```
Virtual LAN ID:100 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interface: FastEthernet0.100

   Protocols Configured: Address: Received: Transmitted:
      IP                 100.0.0.2     10       10

Virtual LAN ID:2500 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interface: FastEthernet0.200

   Protocols Configured: Address: Received: Transmitted:
      IP                 200.0.0.2      5         5
```

Table 4-1 describes the fields shown in the output.

Table 4-1 show vlans Field Descriptions

Field	Description
Virtual LAN ID	Domain number of the VLAN
vLAN Trunk Interface	Subinterface that carries the VLAN traffic
Protocols Configured	Protocols configured on the VLAN
Address	Network address
Received	Packets received
Transmitted	Packets transmitted

CHAPTER 5

Configuring ISDN

This chapter describes how to configure a Cisco router to dial into a central-site router over an ISDN line and provides verification steps and troubleshooting tips.

This chapter contains the following sections:

- Before You Begin
- Dial-Up ISDN Connection to a Central-Site Router
- Dial-Up ISDN Connection with Dialer Profiles
- Leased-Line ISDN Connection to a Central-Site Router
- Dial-In ISDN BRI Pool

Before You Begin

The configurations in this chapter are based on the following assumptions:

- Your Cisco router hardware is correctly installed in accordance with the Hardware Installation Guide for your Cisco router.
- Your Cisco router is using multilink Point-to-Point Protocol (PPP).
- Your ISDN line is installed and correctly configured. Refer to the "Configuring the ISDN Line" chapter in the Hardware Installation Guide for more information on ordering and configuring your ISDN line.

Before you begin configuration, be aware of the following:

- You need to enter the commands in the order shown in the task tables.
- The values shown in italic are examples. For the values shown, you should instead enter values appropriate for your network.
- You should be familiar with Cisco IOS software and its conventions.

Note To use the verification steps described in this chapter, you must be familiar with Cisco IOS commands and command modes. When you use the verification steps, you need to change to different command modes. If you are not familiar with command modes, see the "Understanding Command Modes" section in the "Introduction to Router Configuration" chapter.

Dial-Up ISDN Connection to a Central-Site Router

This section tells how to configure your Cisco router for Internetwork Packet Exchange (IPX) when dialing out over an ISDN line. Configure your router for IP if you want to use Internet services, such as the World Wide Web, or if the network that you are dialing into uses IP. Configure your router for IPX if your network uses IPX network services, such as NetWare file servers or print servers.

This configuration assumes that the Cisco router is dialing into a central-site router.

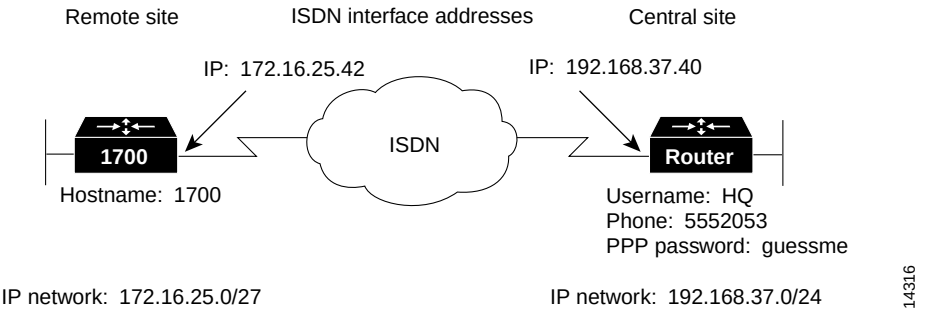
Note If you are using IP but not IPX on your network, do not enter the commands that include the **ipx** keyword.

These are the major tasks in configuring your router:

- Configuring Global Parameters
- Configuring Security
- Configuring the Fast Ethernet Interface
- Configuring the ISDN Interface
- Configuring Static Routes and Dialing Behavior
- Configuring Command-Line Access to the Router

Figure 5-1 shows the configuration example used in this section.

Figure 5-1 ISDN Configuration Example—Dial-Up ISDN Connection to Central Site Router



Configuring Global Parameters

Follow these steps to configure the router for global parameters.

	Command	Task
Step 1	**configure terminal**	Enter configuration mode.
Step 2	**service timestamps debug datetime msec**	Configure the router to show the date and time of all debug messages. This command is optional, but it is recommended if you use debug commands to troubleshoot your configuration.
Step 3	**service timestamps log datetime msec**	Configure the router to show the date and time of all log messages. This command is optional, but it is recommended if you use the verification steps described in this guide. This feature is enabled for all the command output examples shown in this guide.

	Command	Task
Step 4	**isdn switch-type** *basic-ni*	Configure the type of central office switch used on the ISDN interface. Use the keyword that matches the ISDN switch type that you are using: • **basic-1tr6**—German 1TR6 ISDN switches • **basic-5ess**—Basic rate 5ESS switches • **basic-dms100**—NT DMS-100 basic rate switches • **basic-net3**—NET3 ISDN switches • **basic-ni**—National ISDN-1 switches • **basic-nwnet3**—Norway NET3 switches (phase 1) • **basic-nznet3**—New Zealand NET3 switches • **basic-ts013**—Australian TS013 switches • **ntt**—Japanese NTT ISDN switches • **vn2**—French VN2 ISDN switches • **vn3**—French VN3 ISDN switches
Step 5	**ipx routing** *0060.834f.66dd*	(Optional) Enable IPX routing and configure the router with an IPX address.

Configuring Security

Follow these steps to configure the router with security measures.

	Command	Task
Step 1	**enable password** <*user*>	Specify a password to prevent unauthorized access to the router.
Step 2	**hostname** *Router*	Configure the router with a host name, which is used in prompts and default configuration file names. For PPP authentication, the host name entered with this command must match the username of the central-site router.
Step 3	**username** *HQ* **password** <*guessme*>	Specify the password used during caller identification and Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) authentication. For CHAP and PAP authentication, the username entered with this command must match the host name of the central-site router.

Configuring the Fast Ethernet Interface

Follow these steps to configure the Fast Ethernet interface, which connects your router to the local network.

	Command	Task
Step 1	**interface fastethernet0**	Enter configuration mode for the Fast Ethernet interface.
Step 2	**ip address** *172.16.25.42 255.255.255.224*	Configure this interface with an IP address and a subnet mask.
Step 3	**ipx network** *ABC*	(Optional) Enable IPX routing on this interface and assign the interface with an IPX network address.

	Command	Task
Step 4	**no shutdown**	Enable the interface and the configuration changes you have just made on the interface.
Step 5	**exit**	Exit configuration mode for this interface.

Verifying Your Configuration

You can verify your configuration by checking that the Fast Ethernet interface has the correct IP address:

Step 1 From the privileged EXEC command mode, enter the **show arp** command:

```
Router# show arp
```

Step 2 You should see command output similar to the following:

```
Protocol Address          Age (min)   Hardware
Addr    Type   Interface
Internet 171.16.25.42           -     0060.834f.66dd    ARPA   Fast
Ethernet0
Router#
```

Step 3 The IP address, as shown in the command output example, should be your router Fast Ethernet IP address. If it is not, then reenter the IP address with **ip address** interface command.

Step 4 To continue configuration, reenter global configuration mode.

Configuring the ISDN Interface

Follow these steps to configure the ISDN interface, which connects the router to the central-site router over the wide-area network.

	Command	Task
Step 1	**interface BRI0**	Enter configuration mode for the ISDN interface.
Step 2	**description** *ISDN connectivity*	Add a description of this interface to help you remember what is attached to it.
Step 3	**isdn spid1** *555987601*	Enter the service profile identifier (SPID) number assigned by the ISDN service provider to the B1 channel. This step is required only when the service provider has assigned a SPID to your ISDN line. Not all ISDN lines have SPIDs.
Step 4	**isdn spid2** *555987602*	Define the SPID number assigned by the ISDN service provider to the B2 channel. This step is required only when the service provider has assigned a SPID to your ISDN line. Not all ISDN lines have SPIDs.
Step 5	**ip unnumbered fastethernet0**	Enable IP routing on this interface without assigning an IP address.
Step 6	**dialer map ip** *192.168.37.40* **name** *HQ 5552053*	Configure this interface to place a call to multiple sites and to authenticate calls from multiple sites based on IP address and dialer string (phone number). The name you enter after the **name** keyword in this command must match the name entered with the **username** command in the "Configuring Security" section on page 5-4.
Step 7	**ipx network** *123*	(Optional) Enable IPX routing on this interface and assign an IPX network address to the interface.
Step 8	**no ipx route-cache**	(Optional) Disable IPX fast switching on this interface.
Step 9	**ipx watchdog-spoof**	(Optional) Set the router to respond to local server watchdog packets on behalf of a remote client (called *spoofing*).

	Command	Task
Step 10	**dialer map ipx** *123.0000.0003.eccb* **name** *HQ* **broadcast** *5552053*	(Optional) Configure this interface to call multiple sites, based on IPX address and dialer string (phone number).
Step 11	**dialer load-threshold** *70*	Configure bandwidth on demand by setting the maximum load before the router places another call to a destination.
Step 12	**dialer-group** *1*	Assign the dialer interface to a dialer group.
Step 13	**no fair-queue**	Disable weighted fair queuing on this interface.
Step 14	**encapsulation ppp**	Configure this interface for PPP encapsulation.
Step 15	**ppp authentication chap pap**	Enable CHAP and PAP authentication on this interface. CHAP authentication is attempted first. If the central-site router does not support CHAP, then PAP is used for authentication.
Step 16	**ppp multilink**	Enable multilink PPP on this interface.
Step 17	**no shutdown**	Enable the interface and the configuration changes you have just made on the interface.
Step 18	**exit**	Exit configuration mode for this interface.

Verifying Your Configuration

You can verify your configuration to this point by confirming the ISDN line status:

Step 1 From the privileged EXEC command mode, enter the **show isdn status** command.

You should see command output similar to the following:

```
Router# show isdn status
The current ISDN Switchtype = basic-5ess
ISDN BRI0 interface
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 80, State = MULTIPLE_FRAME_ESTABLISHED
```

```
    Layer 3 Status:
        No Active Layer 3 Call(s)
    Activated dsl 0 CCBs = 0
    Total Allocated ISDN CCBs =
```

Step 2 Confirm that the current ISDN switch type matches the actual switch type that you are using. In the output example, the switch type is "basic-5ess."

Step 3 Confirm that the "Layer 1 status: ACTIVE" message appears in the command output. In the output example, the status is "ACTIVE."

Step 4 Confirm that the "State = MULTIPLE_FRAME_ESTABLISHED" message appears in the command output. The output example shows this message.

In some cases, you might see a "State = TEI_ASSIGNED" message instead of the "State = MULTIPLE_FRAME_ESTABLISHED" message. This message also means that the ISDN line is correctly configured.

Step 5 To continue configuration, reenter global configuration mode.

Tips

If you are having problems, do the following:

- Make sure that you entered the **no shutdown** command for the ISDN interface while in interface configuration mode. This enables the configuration changes that you made on the interface.
- Make sure that any external Network Termination 1 (NT1) equipment is functioning correctly. Refer to the documentation that came with the NT1.
- Check with the ISDN service provider to make sure that the ISDN line is correctly configured.

Configuring Static Routes and Dialing Behavior

Follow these steps to configure some parameters that control how and when the router dials the central-site router.

	Command	Task
Step 1	**ip route** *0.0.0.0 0.0.0.0 192.168.37.40*	Establish a static IP route to the remote network.
Step 2	**ip route** *192.168.37.40 255.255.255.255* **BRI0**	Establish a static IP route to the central-site router through this interface.
Step 3	**access-list** *101 permit icmp any any*	Define a standard access list based on Internet Control Message Protocol (ICMP) traffic.
Step 4	**access-list** *101 permit ip any any*	Define a standard access list based on IP traffic.
Step 5	**dialer-list** *1* **protocol ip list** *101*	Specify a dialer list both by list number and by protocol (IP) to define the packets of interest that can trigger a call to the destination.
Step 6	**access-list** *900 deny any any all any 457*	(Optional) Define a standard access list based on IPX network variables.
Step 7	**access-list** *900 deny rip any rip any rip*	(Optional) Define a standard access list based on IPX network variables.
Step 8	**access-list** *deny sap and sap any sap*	(Optional) Define a standard access list based on IPX network variables.
Step 9	**access-list** *900 permit any any all any all*	(Optional) Define a standard access list based on IPX network variables.
Step 10	**dialer-list** *1* **protocol ipx list** *900*	(Optional) Specify an access list both by list number and by protocol (IPX) to define the packets that will trigger the router to make a call to the destination.

Verifying Your Configuration

You can verify your configuration to this point by

- Confirming the Static IP Route
- Confirming the IPX Route
- Confirming Connectivity to the Central-Site Router
- Confirming Multilink PPP Configuration for the B1 Channel
- Confirming Multilink PPP Configuration for the B2 Channel

Confirming the Static IP Route

You can verify your configuration by confirming the static IP route:

Step 1 From the privileged EXEC command mode, enter the **show ip route** command.

Substitute the IP address of the central-site router ISDN interface for the IP address shown in the example.

Step 2 Confirm that the "directly connected via BRI" message (shown in the output example) appears in the command output:

```
Router# show ip route 192.168.37.40
Routing entry for 192.168.37.40/32
  Known via "connected", distance 0, metric 0 (connected)
  Routing Descriptor Blocks:
 * directly connected, via BRI0
      Route metric is 0, traffic share count is 1
```

Step 3 To continue configuration, reenter global configuration mode.

Confirming the IPX Route

Step 1 From the privileged EXEC command mode, enter the **show ipx route** command. You should see command output similar to the following:

```
Router# show ipx route 123
Codes: C - Connected primary network,    c - Connected secondary
network
       S - Static, F - Floating static, L - Local (internal), W -
IPXWAN
```

```
        R - RIP, E - EIGRP, N - NLSP, X - External, A - Aggregate
        s - seconds, u - uses

2 Total IPX routes. Up to 1 parallel paths and 16 hops allowed.

No default route known.

C        123 (PPP),           BR0
```

Step 2 Confirm that the IPX network number (123, in this example) matches the IPX network number that you configured with the **ipx network** command when you configured the Fast Ethernet interface.

Step 3 To continue configuration, reenter global configuration mode.

Confirming Connectivity to the Central-Site Router

You can verify your configuration by confirming connectivity to the central-site router:

Step 1 From the privileged EXEC command mode, enter the **ping** command, followed by the IP address of the central-site router. You should see command output similar to the following:

```
Router# ping 192.168.37.40
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.37.40, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 40/43/48 ms
Router#
*Mar  1 03:37:46.526: %LINK-3-UPDOWN: Interface BRI0:1, changed state
to up
*Mar  1 03:37:46.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface
BRI0:1, changed state to up
*Mar  1 03:37:46.939: %LINK-3-UPDOWN: Interface Virtual-Access1,
changed state to up
*Mar  1 03:37:47.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access1, changed state to up
 *Mar  1 03:35:57.217: %ISDN-6-CONNECT: Interface BRI0:1 is now
connected to 5552053 HQ
```

Step 2 Note the percentage in the “Success rate” line. If the success rate is 60 percent (3/5) or greater, your router is successfully transferring data to the central-site router.

Step 3 To continue configuration, reenter global configuration mode.

Confirming Multilink PPP Configuration for the B1 Channel

Perform the two verification procedures in this section to verify that multilink PPP is configured on the ISDN B1 channel.

For the first verification procedure, perform these steps:

Step 1 From the privileged EXEC mode, confirm that the ISDN is connected to the remote site by entering the **ping** command, followed by the IP address of the central-site router:

```
Router# ping 192.168.37.40
```

Step 2 Enter the **show ppp multilink** command.

Step 3 Confirm that the "Master link is Virtual-Access1" message appears in the command output.

```
Router# show ppp multilink
 Bundle HQ, 1 member, Master link is Virtual-Access1
Dialer Interface is BRI0
  0 lost fragments, 0 reordered, 0 unassigned, sequence 0x0/0x0
rcvd/sent
  0 discarded, 0 lost received, 1/255 load
Member Link: 1
BRI0:1
```

Step 4 If you do not see the message in the output, do one or both of the following:

- Confirm that multilink PPP is configured on the central-site router that you are connecting to.
- If multilink PPP is configured on the central-site router, use the **show interface** command as described in the second verification procedure.

Step 5 To continue configuration, reenter global configuration mode.

For the second verification procedure, perform these steps:

Step 1 From the privileged EXEC command mode, confirm that the ISDN line is connected to the remote site by entering the **ping** command, followed by the IP address of the central-site router:

```
Router# ping 192.168.37.40
```

Step 2 Enter the **show interface virtual-access 1** command.

Step 3 Confirm that the "Open: IPCP" message appears in the command output:

```
Router# show interface virtual-access 1

Virtual-Access1 is up, line protocol is up
  Hardware is Virtual Access interface
  MTU 1500 bytes, BW 64 Kbit, DLY 100000 usec, rely 255/255, load
1/255
  Encapsulation PPP, loopback not set, keepalive set (10 sec)
  DTR is pulsed for 5 seconds on reset
  LCP Open, multilink Open
Open: IPCP
Last input 00:00:01, output never, output hang never
  Last clearing of "show interface" counters 00:54:41
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     708 packets input, 150742 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     709 packets output, 157653 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

Step 4 To continue configuration, reenter global configuration mode.

Confirming Multilink PPP Configuration for the B2 Channel

Perform the two procedure in this section to verify that multilink PPP is configured on the ISDN B2 channel.

Step 1 From the privileged EXEC command mode, confirm that the ISDN line is connected to the remote site by entering the **ping** command, followed by the IP address of the central-site router:

```
Router# ping 192.168.37.40
```

Step 2 Create enough network traffic so that the second ISDN B channel dials the remote site.

Note One way to perform Step 2 is to reduce the amount of data needed to cause the second B channel to dial. To reduce the amount (called the *threshold*), use the **dialer load-threshold** command, which is described in Step 11 of the "Configuring the ISDN Interface" section on page 5-6.

Step 3 Check LEDs B1 and B2.

If both LEDs are lit solid, multilink PPP is correctly configured for both ISDN B channels.

Step 4 To continue configuration, reenter global configuration mode.

Tips

If you are having problems, do the following:

- Confirm that your router is configured with the correct IP address.
- Confirm that you have correctly configured the static IP routes with the **ip route** command.

Configuring Command-Line Access to the Router

Follow these steps to configure some parameters that control access to the router.

	Command	Task
Step 1	**line console** *0*	Specify the console terminal line.
Step 2	**exec-timeout** *5*	Set the interval that the EXEC command interpreter waits until user input is detected.
Step 3	**line vty** *0 4*	Specify a virtual terminal for remote console access.
Step 4	**password** *<lineaccess>*	Specify a password on the line.
Step 5	**login**	Enable password checking at terminal session login.
Step 6	**end**	Exit configuration mode.

Troubleshooting

If you are having problems or the if output that you received during the verification steps is very different from that shown in the command output examples, you can troubleshoot your router, using the Cisco IOS **debug** commands. The **debug** commands provide extensive command output that is not included in this document.

Caution If you are not familiar with Cisco IOS debug commands, you should read the "Using Debug Commands" section in the "Introduction to Router Configuration" chapter before attempting any debugging.

Following are debug commands that are helpful when troubleshooting ISDN with IP routing. Follow these commands with the **ping** command to display the debug output:

- **debug dialer events**
- **debug isdn events**
- **debug isdn q931**

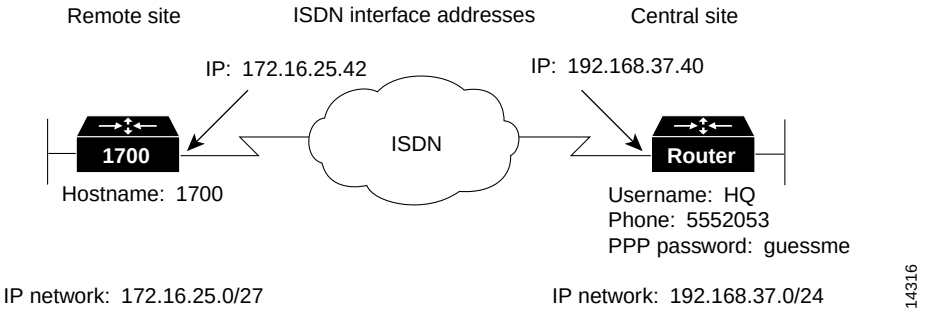
- **debug isdn q921**
- **debug ppp negotiation**
- **debug ppp authentication**
- **debug ppp multilink events**

Dial-Up ISDN Connection with Dialer Profiles

This section describes how to configure dialer profiles for ISDN. If you followed the instructions for configuring ISDN in the previous sections of this chapter, you might not have to perform all of the steps shown in this section.

Figure 5-2 shows the configuration example used in this section.

Figure 5-2 ISDN Configuration Example—Dial-Up ISDN Connection with Dialer Profiles



These are the major tasks in configuring your router:

- Configuring Global Parameters
- Configuring Security
- Configuring the Fast Ethernet Interface
- Configuring the ISDN Interface
- Configuring the Dialer Interface
- Configuring When the Router Dials Out
- Configuring Command-Line Access to the Router

Configuring Global Parameters

Follow these steps to configure the router for global parameters.

	Command	Task
Step 1	**configure terminal**	Enter configuration mode.
Step 2	**service timestamps debug datetime msec**	Configure the router to show the date and time of all debug messages. This command is optional, but it is recommended if you use debug commands to troubleshoot your configuration.
Step 3	**service timestamps log datetime msec**	Configure the router to show the date and time of all log messages. This command is optional, but it is recommended if you use the verification steps described in this guide. This feature is enabled for all the command output examples shown in this guide.

	Command	Task
Step 4	**isdn switch-type** *basic-ni*	Configure the type of central office switch being used on the ISDN interface. Use the keyword that matches the ISDN switch type that you are using: • **basic-1tr6**—German 1TR6 ISDN switches • **basic-5ess**—Basic rate 5ESS switches • **basic-dms100**—NT DMS-100 basic rate switches • **basic-net3**—NET3 ISDN switches • **basic-ni**—National ISDN-1 switches • **basic-nwnet3**—Norway NET3 switches (phase 1) • **basic-nznet3**—New Zealand NET3 switches • **basic-ts013**—Australian TS013 switches • **ntt**—Japanese NTT ISDN switches • **vn2**—French VN2 ISDN switches • **vn3**—French VN3 ISDN switches

Verifying Your Configuration

You can verify your configuration to this point by checking the ISDN line status as follows:

Step 1 From the privileged EXEC command mode, enter the **show isdn status** command.

You should see command output similar to the following:

```
Router# show isdn status
The current ISDN Switchtype = basic-5ess
ISDN BRI0 interface
    Layer 1 Status:
        ACTIVE
```

```
Layer 2 Status:
    TEI = 80, State = MULTIPLE_FRAME_ESTABLISHED
Layer 3 Status:
    No Active Layer 3 Call(s)
Activated dsl 0 CCBs = 0
Total Allocated ISDN CCBs =
```

Step 2 Confirm that the current ISDN switch type matches the actual switch type that you are using.

Step 3 Confirm that the "Layer 1 status: ACTIVE" message appears in the command output, as shown in the output example.

Step 4 Confirm that the "State = MULTIPLE_FRAME_ESTABLISHED" message appears in the command output, as shown in the output example.

Note In some cases, you might see a "State = TEI_ASSIGNED" message instead of the "State = MULTIPLE_FRAME_ESTABLISHED" message. This message also means that the ISDN line is correctly configured.

Step 5 To continue configuration, reenter global configuration mode.

Tips

If you are having problems, do the following:

- Make sure that any external NT1 is functioning correctly. Refer to the documentation that came with the NT1.
- Check with the ISDN service provider to make sure that the ISDN line is correctly configured.

Configuring Security

Follow these steps to configure the router with security measures.

	Command	Task
Step 1	**hostname** *Router*	Configure the router with a host name, which is used in prompts and default configuration filenames. For PPP authentication, the host name entered with this command must match the username of the central-site router.
Step 2	**enable password** <*user*>	Specify a password to prevent unauthorized access to the router.
Step 3	**username** *HQ* **password** <*guessme*>	Specify the password that will be used during CHAP caller identification and PAP. For PPP authentication, the username entered with this command must match the host name of the central-site router.

Configuring the Fast Ethernet Interface

Follow these steps to configure the Fast Ethernet interface, which connects your router to the local network.

	Command	Task
Step 1	**interface fastethernet0**	Enter configuration mode for the Fast Ethernet interface.
Step 2	**ip address** *172.16.25.42 255.255.255.224*	Configure this interface with an IP address and a subnet mask.
Step 3	**ipx network** *ABC*	Enable IPX routing on this interface.
Step 4	**no shutdown**	Enable the interface and the configuration changes you have just made on the interface.
Step 5	**exit**	Exit configuration mode for this interface.

Configuring the ISDN Interface

Follow these steps to configure the ISDN interface, which connects the router to the central-site router over the wide-area network.

	Command	Task
Step 1	**interface BRI0**	Enter configuration mode for the ISDN interface.
Step 2	**description** *ISDN connectivity*	Add a description of the ISDN interface to help you remember what is attached to it.
Step 3	**isdn spid1** *555987601*	Enter the SPID number that has been assigned by the ISDN service provider for the B1 channel. This step is required only when the service provider has assigned a SPID to your ISDN line. Not all ISDN lines required SPIDs.
Step 4	**isdn spid2** *555987602*	Define the SPID number that has been assigned by the ISDN service provider for the B2 channel. This step is required only when the service provider has assigned a SPID to your ISDN line. Not all ISDN lines required SPIDs.
Step 5	**no ip address**	Disable IP routing on this interface.
Step 6	**dialer pool-member** *1*	Put this interface in a dialing pool. As an option, you can also assign a priority to the interface with this command.
Step 7	**encapsulation ppp**	Set the encapsulation method on this interface to PPP.
Step 8	**ppp authentication chap pap**	Enable CHAP and PAP authentication on this interface. CHAP authentication is attempted first. If the central-site router does not support CHAP, then PAP is used for authentication.
Step 9	**ppp multilink**	Enable multilink PPP on this interface.

	Command	Task
Step 10	**no shutdown**	Enable the interface and the configuration changes you have just made on the interface.
Step 11	**exit**	Exit configuration mode for this interface.

Configuring the Dialer Interface

Follow these steps to create a dialer interface and configure it for dial-on-demand routing (DDR).

	Command	Task
Step 1	**interface** *Dialer10*	Create a dialer interface.
Step 2	**ip unnumbered fastethernet0**	Enable IP routing on this interface without assigning an IP address.
Step 3	**ipx network** *123*	Enable IPX routing on this interface.
Step 4	**no ipx route-cache**	Disable IPX fast switching on this interface.
Step 5	**ipx watchdog-spoof**	Set the router to respond to a local server watchdog packets on behalf of a remote client (called *spoofing*).
Step 6	**dialer remote-name** *HQ*	Specify the central-site router CHAP authentication name.
Step 7	**dialer string** *5552053*	Specify the string (telephone number) to be called for this interface when calling a single site.
Step 8	**dialer pool** *1*	Put this interface in a dialing pool. As an option, you can also assign a priority to the interface with this command.
Step 9	**dialer-group** *1*	Assign the dialer interface to a dialer group.
Step 10	**encapsulation ppp**	Set the encapsulation method on this interface to PPP.

	Command	Task
Step 11	**ppp authentication chap pap**	Enable CHAP and PAP authentication on this interface. CHAP authentication is attempted first. If the central-site router does not support CHAP, then PAP is used for authentication.
Step 12	**ppp multilink**	Enable multilink PPP on this interface.
Step 13	**no shutdown**	Enable the interface and the configuration changes you have just made on the interface.
Step 14	**exit**	Exit configuration mode for this interface.

Verifying Your Configuration

You can verify your configuration to this point by confirming the Multilink PPP Configuration for the B1 Channel.

Step 1 Confirm that the ISDN is up and connected to the central-site router.

Step 2 From the privileged EXEC command mode, enter the **show ppp multilink** command.

Step 3 Confirm that the "Master link is Virtual-Access1" message appears in the command output, as shown in the output example.

```
Router# show ppp multilink
 Bundle HQ, 1 member, Master link is Virtual-Access1
Dialer Interface is BRI0
  0 lost fragments, 0 reordered, 0 unassigned, sequence 0x0/0x0
rcvd/sent
  0 discarded, 0 lost received, 1/255 load
Member Link: 1
BRI0:1
```

Step 4 Return to the privileged EXEC command mode, and enter the **show interface** command.

Step 5 Confirm that the "LCP Open, multilink Open" message appears in the command output, as shown in the output example.

```
Router# show interface bri 0 1 2
BRI0:1 is up, line protocol is up
  Hardware is BRI with U interface and external S bus interface
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load
3/255
```

```
  Encapsulation PPP, loopback not set, keepalive set (10 sec)
 LCP Open, multilink Open
Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo...
```

Step 6 To continue configuration, reenter global configuration mode.

Configuring When the Router Dials Out

Follow these steps to configure parameters that control how and when the router dials the central-site router.

	Command	Task
Step 1	**ip route** *192.168.37.0 255.255.255.0 192.168.37.40*	Establish a static IP route to the remote network.
Step 2	**ip route** *192.168.37.40 255.255.255.255 BRI0*	Establish a static IP route to the remote network through the router BRI.
Step 3	**access-list** *101 permit icmp any any*	Define a standard access list based on your network.
Step 4	**access-list** *101 deny ip any any*	Define a standard access list based on your network.
Step 5	**access-list** *900 deny any any all any 457*	Define a standard access list based on your network.
Step 6	**access-list** *900 deny rip any rip any rip*	Define a standard access list based on your network.
Step 7	**access-list** *900 deny sap any sap any sap*	Define a standard access list based on your network.
Step 8	**access-list** *900 permit any any all any all*	Define a standard access list based on your network.

	Command	Task
Step 9	**dialer-list 1 protocol ip list** *101*	Specify an access list both by list number and by protocol (IP) to define the packets of interest that can trigger a call to the destination.
Step 10	**dialer-list 1 protocol ipx list** *900*	Specify an access list both by list number and by protocol (IPX) to define the packets of interest that can trigger a call to the destination.

Verifying Your Configuration

You can verify your configuration to this point by

- Confirming the IP Static Route
- Confirming Connectivity to the Central-Site Router

Confirming the IP Static Route

You can verify your configuration to this point by checking the static IP route as follows:

Step 1 From the privileged EXEC command mode, enter the **show ip route** command.

Substitute the IP address of the central-site router ISDN interface for the IP address shown in the example.

Step 2 Confirm that the "directly connected via BRI" message appears, as shown in the command output.

```
Router# show ip route 192.168.37.40
Routing entry for 192.168.37.40/32
  Known via "connected", distance 0, metric 0 (connected)
  Routing Descriptor Blocks:
 * directly connected, via BRI0
```

Step 3 To continue configuration, reenter global configuration mode.

Confirming Connectivity to the Central-Site Router

You can verify your configuration to this point by testing connectivity to the central-site router, as follows:

Step 1 From the privileged EXEC command mode, enter the **ping** command, followed by the IP address of the central-site route to have the router dial the central-site router. You should see output similar to the following:

```
Router# ping 192.168.37.40

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.37.40, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 40/43/48 ms
Router#
*Mar  1 03:37:46.526: %LINK-3-UPDOWN: Interface BRI0:1, changed state
to up
*Mar  1 03:37:46.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface
BRI0:1, changed state to up
*Mar  1 03:37:46.939: %LINK-3-UPDOWN: Interface Virtual-Access1,
changed state to up
*Mar  1 03:37:47.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access1, changed state to up
 *Mar  1 03:35:57.217: %ISDN-6-CONNECT: Interface BRI0:1 is now
connected to 5552053 HQ
```

Step 2 Wait for the “ISDN-6-CONNECT” message, as shown in the commmand output example.

Step 3 Enter the **ping** command, followed by the IP address of the central-site router again:

```
Router# ping 192.168.37.40

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.37.40, timeout is 2 seconds:
.!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/43/48
ms
Router#
*Mar  1 03:37:46.526: %LINK-3-UPDOWN: Interface BRI0:1, changed state
to up
*Mar  1 03:37:46.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface
BRI0:1, changed state to up
*Mar  1 03:37:46.939: %LINK-3-UPDOWN: Interface Virtual-Access1,
changed state to up
```

```
*Mar  1 03:37:47.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access1, changed state to up
 *Mar  1 03:35:57.217: %ISDN-6-CONNECT: Interface BRI0:1 is now
connected to 5552053 HQ
```

If the success rate, as shown in the command output, is 100 percent, this verification step is successful.

Step 4 To continue configuration, reenter global configuration mode.

Tips

If you are having problems, do the following:

- Make sure that the router is configured with the correct IP address.
- Make sure that the router is configured with the correct static routes.

Configuring Command-Line Access to the Router

Follow these steps to configure parameters that control access to the router, such as what type of terminal line can be used with the router, how long the user has to input a command before the router times out, and what password is used to start a terminal session with the router.

	Command	Task
Step 1	**line console** *0*	Specify the console terminal line.
Step 2	**exec-timeout** *5*	Set the interval that the EXEC command interpreter waits until user input is detected.
Step 3	**line vty** *0 4*	Specify a virtual terminal for remote console access
Step 4	**password** *<lineaccess>*	Specify a password on the line.
Step 5	**login**	Enable password checking at terminal session login.
Step 6	**end**	Exit configuration mode.

Troubleshooting Dialer Profile Problems

If you are having problems, or if the output that you received during the verification steps is very different from that shown in the command output examples, you can troubleshoot your router, using the Cisco IOS **debug** commands. The **debug** commands provide extensive command output that is not included in this document.

Caution If you are not familiar with Cisco IOS debug commands, you should read the "Using Debug Commands" section in the "Introduction to Router Configuration" chapter before attempting any debugging.

The following are debug commands that are helpful in troubleshooting dialer profiles with ISDN. You need to follow most of these commands with the **ping** command to display debug output:

- **debug dialer**
- **debug isdn events**
- **debug dialer events**
- **debug isdn q931**
- **debug isdn q921**
- **debug ppp negotiation**
- **debug ppp authentication**
- **debug ppp multilink events**

Leased-Line ISDN Connection to a Central-Site Router

This section describes how to configure the router so that it uses the ISDN line as a leased-line connection to the central-site router. Unlike a switched connection to the central-site router, in which the router dials the central-site router only when it detects specified types and amounts of data traffic, a leased-line ISDN connection is always connected to the central office switch.

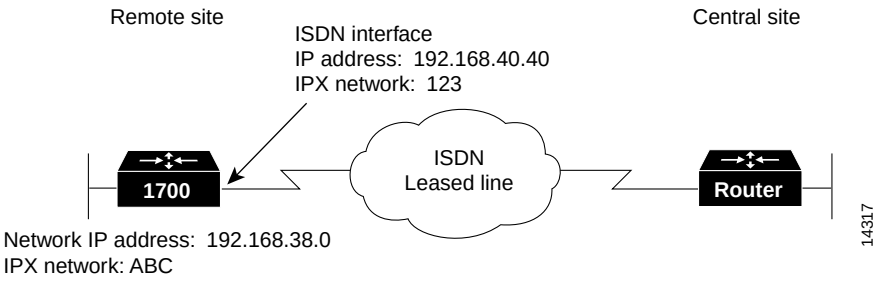
In addition to the assumptions described in the "Before You Begin" section at the beginning of this chapter, this configuration is based on the additional assumption that both ISDN B channels are connecting to the same central-site router.

These are the major tasks in configuring your router for a leased-line ISDN connection:

- Configuring Global Parameters
- Configuring Security
- Configuring IPX Routing
- Configuring the ISDN Line for Leased Line
- Configuring the Fast Ethernet Interface
- Clearing the ISDN Interface
- Configuring the ISDN Subinterfaces
- Configuring Dynamic IP Routing
- Configuring Command-Line Access to the Router

Figure 5-3 shows the configuration example that is used in this section.

Figure 5-3 ISDN Configuration Example—Leased-Line Connection to a Central-Site Router



Configuring Global Parameters

Follow these steps to configure the router for global parameters.

	Command	Task
Step 1	**configure terminal**	Enter configuration mode.
Step 2	**service timestamps debug datetime msec**	Configure the router to show the date and time of all debug messages. This command is optional, but it is recommended if you use debug commands to troubleshoot your configuration.
Step 3	**service timestamps log datetime msec**	Configure the router to show the date and time of all log messages. This command is optional, but it is recommended if you use the verification steps described in this guide. This feature is enabled for all the command output examples shown in this guide.

	Command	Task
Step 4	**isdn switch-type** *basic-ni*	Configure the type of central office switch used on the ISDN interface. Use the keyword that matches the ISDN switch type that you are using: • **basic-1tr6**—German 1TR6 ISDN switches • **basic-5ess**—Basic rate 5ESS switches • **basic-dms100**—NT DMS-100 basic rate switches • **basic-net3**—NET3 ISDN switches • **basic-ni**—National ISDN-1 switches • **basic-nwnet3**—Norway NET3 switches (phase 1) • **basic-nznet3**—New Zealand NET3 switches • **basic-ts013**—Australian TS013 switches • **ntt**—Japanese NTT ISDN switches • **vn2**—French VN2 ISDN switches • **vn3**—French VN3 ISDN switches

Configuring Security

Follow these steps to configure the router with security measures.

	Command	Task
Step 1	**enable password** <*user*>	Specify a password to prevent unauthorized access to the router.
Step 2	**hostname** *Router*	Configure the router with a host name, which is used in prompts and default configuration filenames. For PPP authentication, the host name entered with this command must match the username of the central-site router.
Step 3	**username** *HQ* **password** <*guessme*>	Specify the password used during caller identification and CHAP and PAP authentication. For CHAP and PAP authentication, the username entered with this command must match the host name of the central-site router.

Configuring IPX Routing

Perform this step to enable IPX routing on the router. The default setting for the router is "IPX routing disabled."

Command	Task
ipx routing *0060.834f.66dd*	Enable IPX routing, and configure the router with an IPX address.

Configuring the ISDN Line for Leased Line

Follow these steps to set up the ISDN line for a leased-line configuration.

	Command	Task
Step 1	**multilink virtual-template** *1*	Define a virtual template from which this multilink PPP bundle interface can replicate its interface parameters.
Step 2	**isdn leased-line BRI0** *128*	Configure the BRI interface to use the ISDN physical connection as a leased-line service. If you want to combine both B channels into a single data pipe, enter the *128* keyword with this command.

Configuring the Fast Ethernet Interface

Use this table to configure the Fast Ethernet interface, which connects your router to the local network.

	Command	Task
Step 1	**interface fastethernet0**	Enter configuration mode for the Fast Ethernet interface.
Step 2	**ip address** *192.168.38.42 255.255.255.0*	Configure this interface with an IP address and a subnet mask.
Step 3	**ipx network** *ABC*	Configure this interface with an IPX network address.
Step 4	**interface virtual-template***1*	Associate the virtual template with this interface.
Step 5	**ip address** *192.168.40.40 255.255.255.0*	Configure the virtual template interface with an IP address and a subnet mask.
Step 6	**ipx network** *123*	Configure the virtual template interface with an IPX network address.
Step 7	**encapsulation ppp**	Set the encapsulation method on this interface to PPP.
Step 8	**ppp multilink**	Enable multilink PPP on this interface.

	Command	Task
Step 9	**no shutdown**	Enable the interface and the configuration changes you have just made on the interface.
Step 10	**exit**	Exit configuration mode for this interface.

Clearing the ISDN Interface

Follow these steps to clear the IP address from the ISDN interface.

	Command	Task
Step 1	**interface BRI0**	Enter configuration mode for the BRI interface.
Step 2	**no ip address**	Disable IP routing on the BRI0 interface.
Step 3	**exit**	Exit configuration mode for this interface.

Configuring the ISDN Subinterfaces

Follow these steps to create and configure two ISDN subinterfaces, which connect your router to the central-site router over the wide-area network.

	Command	Task
Step 1	**interface BRI0:1**	Enter configuration mode for the BRI0:1 subinterface
Step 2	**ip unnumbered Virtual-Template***1*	Enable IP routing on this interface without assigning an IP address.
Step 3	**encapsulation ppp**	Set the encapsulation method on this interface to PPP.
Step 4	**ppp multilink**	Enable multilink PPP on this interface.
Step 5	**interface BRI0:2**	Enter configuration mode for the BRI0:2 subinterface.

	Command	Task
Step 6	**ip unnumbered Virtual-Template***1*	Enable IP routing on this interface without assigning an IP address.
Step 7	**encapsulation ppp**	Set the encapsulation method on this interface to PPP.
Step 8	**ppp multilink**	Enable multilink PPP on this interface.
Step 9	**exit**	Exit configuration mode for this interface.

Configuring Dynamic IP Routing

Follow these steps to configure the router for dynamic IP routing.

	Command	Task
Step 1	**ip classless**	Configure the router to forward packets addressed to a subnet of a network with no network default route.
Step 2	**ip route 0.0.0.0 0.0.0.0** *192.168.40.41*	Specify dynamic routing.

Verifying Your Configuration

You can verify your configuration by confirming connectivity to the central-site router.

Step 1 From the privileged EXEC command mode, enter the **ping** command, followed by the IP address of the central-site route to have the router dial the central-site router. You should see output similar to the following:

```
Router# ping 192.168.37.40

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.37.40, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 40/43/48 ms
Router#
*Mar  1 03:37:46.526: %LINK-3-UPDOWN: Interface BRI0:1, changed state
to up
```

```
*Mar  1 03:37:46.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface
BRI0:1, changed state to up
*Mar  1 03:37:46.939: %LINK-3-UPDOWN: Interface Virtual-Access1,
changed state to up
*Mar  1 03:37:47.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access1, changed state to up
 *Mar  1 03:35:57.217: %ISDN-6-CONNECT: Interface BRI0:1 is now
connected to 5552053 HQ
```

Step 2 Wait for the "ISDN-6-CONNECT" message, as shown in the command output example.

Step 3 Enter the **ping** command, followed by the IP address of the central-site router again:

```
Router# ping 192.168.37.40

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.37.40, timeout is 2 seconds:
.!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/43/48
ms
Router#
*Mar  1 03:37:46.526: %LINK-3-UPDOWN: Interface BRI0:1, changed state
to up
*Mar  1 03:37:46.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface
BRI0:1, changed state to up
*Mar  1 03:37:46.939: %LINK-3-UPDOWN: Interface Virtual-Access1,
changed state to up
*Mar  1 03:37:47.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access1, changed state to up
 *Mar  1 03:35:57.217: %ISDN-6-CONNECT: Interface BRI0:1 is now
connected to 5552053 HQ
```

If the success rate is 100 percent, this verification step is successful.

Step 4 If the router is not successfully transferring data to the central-site router (if the success rate is less than 60 percent), do the following:

- Use the **show ip route** command to confirm that the routing table entries for the central-site router are correct.
- Use the **show interface bri0** command to confirm that the ISDN interface is active and that IPCP, IPXCP, and Multilink are shown as "Open."

Step 5 To continue configuration, reenter global configuration mode.

Configuring Command-Line Access to the Router

Follow these steps to configure parameters that control access to the router, such as what type of terminal line is used with the router, how long the router waits for a user entry before it times out, and what password is used to start a terminal session with the router.

	Command	Task
Step 1	**ip classless**	Configure the router to forward packets addressed to a subnet of a network with no network default route.
Step 2	**ip route 0.0.0.0 0.0.0.0** *192.168.40.41*	Specify dynamic routing.
Step 3	**ip classless**	Configure the router to forward packets addressed to a subnet of a network with no network default route.
Step 4	**ip route 0.0.0.0 0.0.0.0** *192.168.40.41*	Specify dynamic routing.
Step 5	**ip classless**	Configure the router to forward packets addressed to a subnet of a network with no network default route.
Step 6	**ip route 0.0.0.0 0.0.0.0** *192.168.40.41*	Specify dynamic routing.

Troubleshooting Problems with Leased Lines

If you are having problems or if the output that you received during the verification steps is very different from that shown in the command output examples, you can troubleshoot your router, using the Cisco IOS **debug** commands. The **debug** commands provide extensive command output that is not included in this document.

Caution If you are not familiar with Cisco IOS debug commands, you should read the "Using Debug Commands" section in the "Introduction to Router Configuration" chapter before attempting any debugging.

The following debug commands are helpful in troubleshooting an ISDN leased line. Follow these commands with the **ping** command to display debug output.

- **debug ppp negotiation**
- **debug isdn events**
- **debug q931**
- **debug q921**

Dial-In ISDN BRI Pool

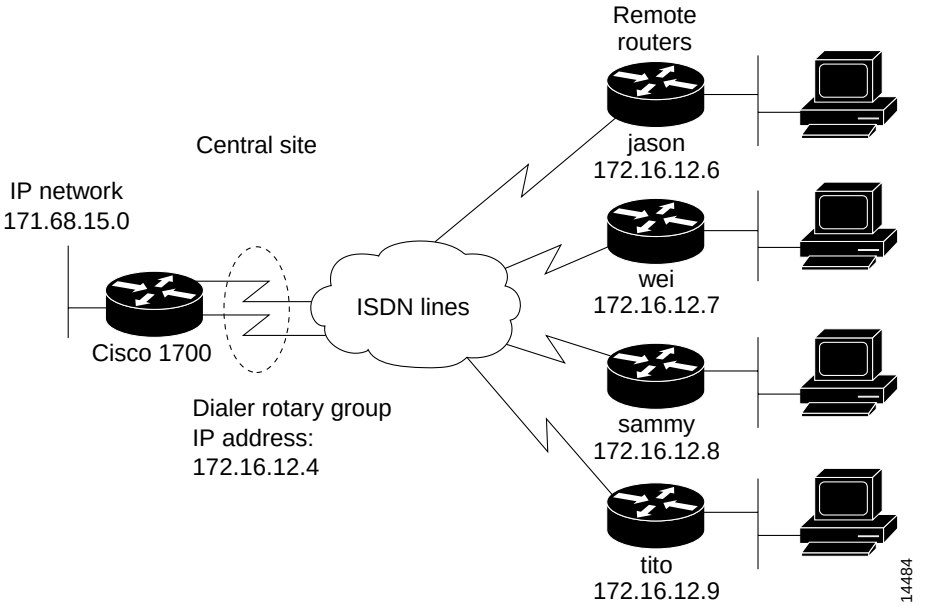
This section describes how to configure a Cisco router with two ISDN BRI interfaces to function as a dial-in server. In this example, the Cisco router functions as the central-site router that accepts dial-in connections from remote routers.

These are the major tasks in configuring your router for dial-in ISDN connections:

- Configuring Global Parameters
- Configuring Security
- Configuring the Fast Ethernet Interface
- Configuring the ISDN Interfaces
- Configuring a Dialer Interface
- Configuring EIGRP Routing
- Configuring IP Static Routes and Dial-In Parameters
- Configuring Command-Line Access to the Router

Figure 5-4 shows the configuration example used in this section.

Figure 5-4 ISDN Configuration Example—Dial-In ISDN BRI Pool



Configuring Global Parameters

Follow these steps to configure global router parameters.

	Command	Task
Step 1	**configure terminal**	Enter configuration mode.
Step 2	**service timestamps debug datetime msec**	Configure the router to show the date and time of all debug messages. This command is optional, but it is recommended if you use debug commands to troubleshoot your configuration.

	Command	Task
Step 3	**service timestamps log datetime msec**	Configure the router to show the date and time of all log messages. This command is optional, but it is recommended if you use the verification steps described in this guide. This feature is enabled for all the command output examples shown in this guide.
Step 4	**isdn switch-type** *basic-ni*	Configure the type of central office switch being used on the ISDN interface. Use the keyword that matches the ISDN switch type that you are using: • **basic-1tr6**—German 1TR6 ISDN switches • **basic-5ess**—Basic rate 5ESS switches • **basic-dms100**—NT DMS-100 basic rate switches • **basic-net3**—NET3 ISDN switches • **basic-ni**—National ISDN-1 switches • **basic-nwnet3**—Norway NET3 switches (phase 1) • **basic-nznet3**—New Zealand NET3 switches • **basic-ts013**—Australian TS013 switches • **ntt**—Japanese NTT ISDN switches • **vn2**—French VN2 ISDN switches • **vn3**—French VN3 ISDN switches

Configuring Security

Follow these steps to configure security measures.

	Command	Task
Step 1	**enable password** <*user*>	Specify a password to prevent unauthorized access to the router.
Step 2	**hostname** *Router*	Configure the router with a host name, which is used in prompts and default configuration filenames. For PPP authentication, the host name entered with this command must match the username of the central-site router.
Step 3	**username** *jason* **password** <*foot*> **username** *wei* **password** <*letmein*> **username** *sammy* **password** <*bar*> **username** *tito* **password** <*knockknock*>	Specify the password used during caller identification and CHAP and PAP authentication. For CHAP and PAP authentication, the host name of every remote router that dials into the Cisco router must be entered with this command, along with the password used to authenticate the router.

Configuring the Fast Ethernet Interface

Follow these steps to configure the Fast Ethernet interface, which connects your router to the local network.

	Command	Task
Step 1	**interface fastethernet0**	Enter configuration mode for this interface.
Step 2	**ip address** *171.68.15.33 255.255.255.248*	Configure this interface with an IP address and a subnet mask.
Step 3	**no shutdown**	Enable this interface and the configuration changes that you have just made.
Step 4	**exit**	Exit configuration mode for this interface.

Configuring the ISDN Interfaces

Follow these steps to configure the two ISDN interfaces that accept calls from remote routers.

	Command	Task
Step 1	**interface BRI0**	Enter configuration mode for the first ISDN interface.
Step 2	**no ip address**	Remove any IP addresses that might be assigned to this interface.
Step 3	**encapsulation ppp**	Configure the interface for PPP packet encapsulation.
Step 4	**dialer rotary-group** *100*	Configure this interface to be included in the dialer rotary group that you will configure in the "Configuring a Dialer Interface" section on page 5-44.
Step 5	**no fair queue**	Disable weighted fair queueing on this interface.
Step 6	**no shutdown**	Enable this interface and the configuration changes you have just made.
Step 7	**exit**	Exit configuration mode for this interface.
Step 8	**interface BRI1**	Enter configuration mode for the second ISDN interface.
Step 9	**no ip address**	Remove any IP addresses that might be assigned to this interface.
Step 10	**encapsulation ppp**	Configure the interface for PPP packet encapsulation.
Step 11	**dialer rotary-group** *100*	Configure this interface to be included in the dialer rotary group that you will configure in the "Configuring a Dialer Interface" section on page 5-44.
Step 12	**no fair queue**	Disable weighted fair queuing on this interface.

	Command	Task
Step 13	**no shutdown**	Enable this interface and the configuration changes you have just made.
Step 14	**exit**	Exit configuration mode for this interface.

Configuring a Dialer Interface

Follow these steps to configure the two ISDN interfaces as one dialer interface that accepts calls from remote routers.

	Command	Task
Step 1	**interface dialer** *100*	Create a dialer rotary group interface, and enter configuration mode for that interface. The number (in this example, 100) is an integer that you select to identify the interface.
Step 2	**ip address** *172.16.12.4 255.255.255.240*	Configure this interface with an IP address.
Step 3	**encapsulation ppp**	Configure this interface for PPP encapsulation.
Step 4	**dialer in-band**	Specify that DDR is supported on this interface.
Step 5	**dialer idle-timeout** *300*	Configure the ISDN line to go down after a specified number of seconds elapses with no network traffic.
Step 6	**dialer map ip** *172.16.12.6* **name** *jason* **broadcast** *5553756* **dialer map ip** *172.16.12.7* **name** *wei* **broadcast** *5553756* **dialer map ip** *172.16.12.8* **name** *sammy* **broadcast** *5553756* **dialer map ip** *172.16.12.9* **name** *tito* **broadcast** *5553756*	Configure this interface to receive and authenticate calls from multiple sites, based on IP address and dialer string. You must enter this command for every remote router that will dial into your router. The name you enter after the **name** keyword in this command must match the name entered with the **username** command in the "Configuring Security" section on page 5-41.

	Command	Task
Step 7	**dialer load-threshold** *70*	Configure bandwidth on demand by setting the maximum load before the router places another call to a destination.
Step 8	**dialer-group** *1*	Assign the dialer interface to a dialer group.
Step 9	**no fair-queue**	Disable weighted fair queuing on this interface.
Step 10	**ppp multilink**	Enable multilink PPP on this interface.
Step 11	**ppp authentication chap**	Enable CHAP or PAP authentication on this interface.
Step 12	**no shutdown**	Enable the dialer interface and the configuration changes that you have just made.
Step 13	**exit**	Exit configuration mode for this interface.

Configuring EIGRP Routing

Follow these steps to configure the router for Enhanced Interior Gateway Routing Protocol (EIGRP) and IP routing parameters that the router uses to connect to the central-site router.

	Command	Task
Step 1	**router eigrp** *109*	Configure the IP EIGRP routing process, and enter router configuration mode.
Step 2	**network** *171.68.0.0*	Specify a list of networks for the EIGRP routing process by entering the IP address of the directly connected network.
Step 3	**redistribute static**	Configure the router to distribute IP static routers from one routing domain to another.
Step 4	**exit**	Exit router configuration mode.

Configuring IP Static Routes and Dial-In Parameters

Follow these steps to configure an IP static router and the access lists that define what type of network traffic the router will accept.

	Command	Task
Step 1	**ip route** *171.68.0.0 255.255.255.240 171.68.12.1*	Configure an IP static route used to route data received from remote routers.
Step 2	**access-list** *101* **deny ip any host 255.255.255.255**	Define a standard access list based on IP network variables.
Step 3	**access-list** *101* **permit ip any any**	Define a standard access list based on IP network variables.
Step 4	**dialer-list** *1* **list** *101*	Specify a dialer list both by list number and by protocol (IP) to define the packets of interest that can trigger a call to the destination.

Configuring Command-Line Access to the Router

Follow these steps to configure parameters that control access to the router, such as what type of terminal line can be used with the router, how long the router waits for a user entry before it times out, and what password is used to start a terminal session with the router.

	Command	Task
Step 1	**line console** *0*	Specify the console terminal line.
Step 2	**exec-timeout** *5*	Set the interval that the EXEC command interpreter waits until user input is detected.
Step 3	**line vty** *0 4*	Specify a virtual terminal for remote console access.
Step 4	**password** *<lineaccess>*	Specify a password on the line.

	Command	Task
Step 5	**login**	Enable password checking at terminal session login.
Step 6	**end**	Exit configuration mode.

CHAPTER 6

Configuring a Leased Line

The configuration in this chapter describes how to configure a Cisco router for IP and Internetwork Packet Exchange (IPX) over a synchronous serial line.

Before You Begin

The configuration in this chapter is based on the following assumptions:

- Your Cisco router hardware is correctly installed in accordance with the Hardware Installation Guide for your Cisco router.
- Your Cisco router is using multilink Point-to-Point Protocol (PPP).
- Your Cisco router is using dynamic IP and IPX routing, in which IP Routing Information Protocol (RIP) resolves IP routes, and IPX RIP and IPX Service Advertising Protocol (SAP) dynamically resolve IPX routes and services.

Before you begin configuration, be aware of the following:

- You need to enter the commands in the order shown in the task tables.
- The values shown in italic are examples. For the values shown, you should instead enter values appropriate for your network.
- You should be familiar with Cisco IOS software and its conventions.

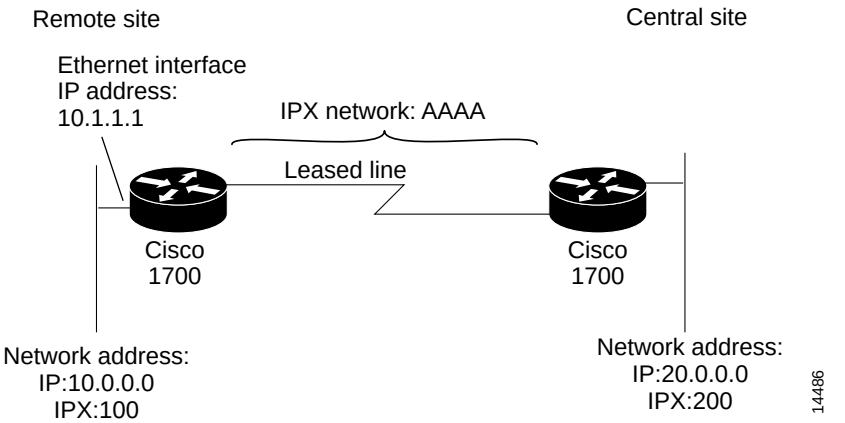
Note To use the verification steps described in this chapter, you must be familiar with Cisco IOS commands and command modes. When you use the verification steps, you need to change to different command modes. If you are not familiar with command modes, see the "Understanding Command Modes" section in the "Introduction to Router Configuration" chapter.

These are the major tasks in configuring the router:

- Configuring Global Parameters
- Configuring Security
- Configuring the Fast Ethernet Interface
- Configuring the Serial Interface
- Configuring Dynamic Routing Parameters
- Configuring Command-Line Access to the Router

Figure 6-1 shows the configuration example used in this chapter.

Figure 6-1 Configuration Example for Leased Line



Configuring Global Parameters

Follow these steps to configure the router for global parameters.

	Command	Task
Step 1	**configure terminal**	Enter configuration mode.
Step 2	**service timestamps debug datetime msec**	Configure the router to show the date and time of all debug messages. This command is optional, but it is recommended if you use debug commands to troubleshoot your configuration.
Step 3	**service timestamps log datetime msec**	Configure the router to show the date and time of all log messages. This command is optional, but it is recommended if you use the verification steps described in this guide. This feature is enabled for all the command output examples shown in this guide.
Step 4	**ip subnet-zero**	Configure the router to use subnet zero for interface addresses and routing updates.
Step 5	**no ip domain-lookup**	Disable the IP Domain Name System (DNS)–based host name–to–address translation on the router.
Step 6	**ipx routing** *0000.0caa.1111*	Enable IPX routing, and configure the router with an IPX address.

Configuring Security

Follow these steps to configure the router with security measures.

	Command	Task
Step 1	**enable password** *<user>*	Specify a password to prevent unauthorized access to the router.
Step 2	**hostname** *Router*	Configure the router with a host name, which is used in prompts and default configuration filenames. For PPP authentication, the host name entered with this command must match the username of the central-site router.

Configuring the Fast Ethernet Interface

Follow these steps to configure the Fast Ethernet interface, which connects your router to the local network.

	Command	Task
Step 1	**interface fastethernet0**	Enter configuration mode for the Fast Ethernet interface.
Step 2	**ip address** *10.1.1.1 255.0.0.0*	Configure this interface with an IP address and a subnet mask. This interface must have an IP address assigned in order for the serial interface to be configured for IP unnumbered routing.
Step 3	**ipx network** *100* **encapsulation sap**	Enable IPX routing on this interface, assign the IPX network number, and configure the interface for IPX SAP encapsulation.
Step 4	**ipx network** *100* **encapsulation novell-ether secondary**	Configure a secondary IPX network that uses the default NetWare encapsulation.
Step 5	**no shutdown**	Enable the interface and the configuration changes you have just made on the interface.
Step 6	**exit**	Exit configuration mode for this interface.

Configuring the Serial Interface

Follow these steps to configure the serial interface, which connects your router to the central-site router.

	Command	Task
Step 1	**interface serial0**	Enter configuration mode for the serial interface.
Step 2	**description** *leased line to headquarters*	Add a description of this interface to help you remember what is attached to it.
Step 3	**ip unnumbered FastEth0**	Enable IP routing on this interface without assigning an IP address.
Step 4	**ipx network** *AAAA*	Enable IPX routing on this interface, and assign an IPX network number.
Step 5	**encapsulation PPP**	Configure this interface for PPP encapsulation.
Step 6	**no shutdown**	Enable this interface and the configuration changes you have just made on the interface.
Step 7	**exit**	Exit configuration mode for this interface.

Configuring Dynamic Routing Parameters

Follow these steps to configure some dynamic routing parameters.

	Command	Task
Step 1	**router rip**	Enable RIP routing on the router, and enter router configuration mode.
Step 2	**version 2**	Specify the router to use RIP version 2.
Step 3	**network** *10.0.0.0*	Enable Enhanced Interior Gateway Routing Protocol (EIGRP) for this network.
Step 4	**no auto-summary**	Disable automatic summarization of subnet routes into network-level routes.

	Command	Task
Step 5	**ip classless**	Configure the router to forward packets addressed to a subnet of a network with no network default route.
Step 6	**exit**	Exit router configuration mode.

Configuring Command-Line Access to the Router

Follow these steps to configure parameters that control access to the router.

	Command	Task
Step 1	**line console** *0*	Specify the console terminal line, and enter line configuration mode.
Step 2	**exec-timeout** *5*	Set the interval that the EXEC command interpreter waits until user input is detected.
Step 3	**line vty** *0 4*	Specify a virtual terminal for remote console access.
Step 4	**password** *<lineaccess>*	Specify a password on the line.
Step 5	**login**	Enable password checking at terminal session login.
Step 6	**end**	Exit configuration mode.

Verifying Your Configuration

You can verify your configuration by checking the serial interface configuration:

Step 1 From privileged EXEC command mode, enter the **show interface serial0** command. You should see output similar to the following:

```
Router# show interface ser0
Serial0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Description: leased line to headquarters
  Interface is unnumbered.  Using address of FastEthernet0 (10.1.1.1)
```

```
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load
1/255
  Encapsulation PPP, loopback not set, keepalive set (10 sec)
  LCP Closed
.
.
.
```

Step 2 Confirm that the "Serial0 is up, line protocol is up" message appears, as shown in the command output example.

Step 3 Proceed as appropriate:

- If you see the "Serial0 is up, line protocol is up" message shown in the example command output, continue configuration by reentering global configuration mode.
- If you see one of the following messages instead of the "Serial0 is up, line protocol is up" message, see the "Troubleshooting Problems with Leased Lines" section for possible causes of the message and suggested actions:
  - Serial0 is down, line protocol is down.
  - Serial0 is up, line protocol is down.
  - Serial0 is up, line protocol is up (looped).
  - Serial0 is administratively down, line protocol is up.

Troubleshooting Problems with Leased Lines

Table 6-1 describes some common problems with leased lines, possible causes, and suggested actions for solving the problems. The table uses Serial 0 port as the location of the problems.

Table 6-1 Possible Causes of and Suggested Actions for Solving Problems with Leased Lines

Line State	Possible Cause	Suggested Actions
Serial0 is down, line protocol is down.	The router is not sensing a Carrier Detect (CD) signal as a result of one of the following: • Telephone company problem, such as the line is down or not connected to the data service unit / channel service unit (DSU/CSU). • Faulty or incorrect cabling of the router. • Local DSU/CSU hardware failure. • Local router hardware failure.	The following are some steps you can take to isolate the problem: • Check the LEDs on the external DSU/CSU for CD activity. • Refer to the Hardware Installation Guide to confirm that your router is correctly installed, using the appropriate cables. • Contact the telephone company to determine if the leased line is down or not connected. • Connect the leased line to another port, if possible. If the connection comes up, there is a hardware failure on the Serial 0 port. Contact your Cisco reseller.
Serial0 is up, line protocol is down.	Possible causes for this line state are • Local or remote router misconfigured. • The remote router is not sending keepalive packets. • Problem with the leased line. • The serial clock transmit external is not set on the DSU/CSU. • Local or remote DSU/CSU hardware failure. • Router hardware failure.	The following are some steps you can take to isolate the problem: • Perform DSU/CSU loopback tests. During local loopback, enter the **show interface ser0** command. If the line protocol is shown as up, there might be a problem with the telephone company, or the remote router might be down. • Refer to the Hardware Installation Guide to confirm that your router is correctly installed, using the appropriate cables. • Connect the leased line to another port, if possible. If the connection comes up, there is a hardware failure on the Serial 0 port. Contact your Cisco reseller.

Table 6-1 Possible Causes of and Suggested Actions for Solving Problems with Leased Lines

Line State	Possible Cause	Suggested Actions
Serial0 is up, line protocol is up (looped).	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.	The 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 whether the DSU/CSU is configured in manual loopback mode. If it is, disable manual loopback. • Reset the DSU/CSU. • If you are unable to isolate the problem, contact the telephone company for help with troubleshooting.
Serial0 is administratively down, line protocol is up.	The possible causes for this state are • The serial interface has been disabled with the **shutdown interface** configuration command. • Different interfaces on the router are using the same IP address.	The following are some steps you can take to isolate the problem: • Use the **show configuration** privileged EXEC command to display the serial port configuration. If "shutdown" is displayed after "interface Serial0," use the **no shutdown** interface configuration command to enable the interface. • Use the **show interface** privileged EXEC command to display the IP addresses for all router interfaces. Use the **ip address** interface configuration command to assign unique IP addresses to the router interfaces.

CHAPTER 7

Configuring Frame Relay

This chapter tells how to configure the Cisco router to connect to a central-site router over a a Frame Relay line and provides verification steps and troubleshooting tips.

This chapter contains the following sections:

- Before You Begin
- Frame Relay
- Frame Relay with an Internal DSU/CSU
- ISDN as the Backup WAN Connection
- ISDN as a Backup Connection with Dialer Profiles
- ISDN as a Backup Connection with Floating Static Routes

Before You Begin

The configurations in this chapter are based on the following assumptions:

- Your Cisco router hardware is correctly installed in accordance with the Hardware Installation Guide for your Cisco router.
- Your Cisco router is connected to a central-site router over Frame Relay.
- Your Cisco router is using multilink Point-to-Point Protocol (PPP).

Before you begin configuration, be aware of the following:

- You need to enter the commands in the order shown in the task tables.
- The values shown in italic are examples. For the values shown, you should instead enter values appropriate for your network.
- You should be familiar with Cisco IOS software and its conventions.

Note To use the verification steps described in this chapter, you must be familiar with Cisco IOS commands and command modes. When you use the verification steps, you need to change to different command modes. If you are not familiar with command modes, see the "Understanding Command Modes" section in the "Introduction to Router Configuration" chapter.

Frame Relay

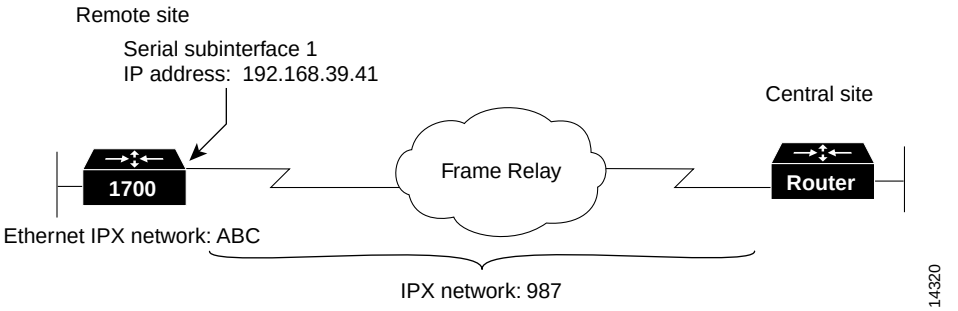
This section describes how to configure a basic Frame Relay connection to the central-site router.

These are the major tasks in configuring your router:

- Configuring Global Parameters
- Configuring Security
- Configuring the Fast Ethernet Interface
- Configuring the Serial Interface for a Frame Relay Connection
- Configuring the Point-to-Point Frame Relay Connection
- Configuring Routing Parameters

Figure 7-1 shows the configuration example used in this section.

Figure 7-1 Configuration Example—Frame Relay



Configuring Global Parameters

Follow these steps to configure the router for global parameters.

	Command	Task
Step 1	**configure terminal**	Enter configuration mode.
Step 2	**service timestamps debug datetime msec**	Configure the router to show the date and time of all debug messages. This command is optional, but it is recommended if you use debug commands to troubleshoot your configuration.
Step 3	**service timestamps log datetime msec**	Configure the router to show the date and time of all log messages. This command is optional, but it is recommended if you use the verification steps described in this guide. This feature is enabled for all the command output examples shown in this guide.
Step 4	**ipx routing** *0060.834f.66dd*	Enable Internetwork Packet Exchange (IPX) routing, and configure the router with an IPX address.

Configuring Security

Follow these steps to configure the router with security measures.

	Command	Task
Step 1	**hostname** *Router*	Configure the router with a host name, which is used in prompts and default configuration filenames. For PPP authentication, the host name entered with this command must match the username of the central-site router.
Step 2	**enable password** <*user*>	Specify a password to prevent unauthorized access to the router.

Configuring the Fast Ethernet Interface

Follow these steps to configure the Fast Ethernet interface, which connects your router to the local network.

	Command	Task
Step 1	**interface fastethernet0**	Enter configuration mode for the Fast Ethernet interface.
Step 2	**ip address** *172.16.25.1 255.255.255.0*	Configure this interface with an IP address and a subnet mask.
Step 3	**ipx network** *ABC*	Enable IPX routing on this interface.
Step 4	**no shutdown**	Enable the interface and the configuration changes that you have just made on the interface.
Step 5	**exit**	Exit configuration mode for this interface.

Configuring the Serial Interface for a Frame Relay Connection

Follow these steps to configure the serial interface for Frame Relay packet encapsulation.

	Command	Task
Step 1	**interface Serial0**	Enter configuration mode for the serial interface.
Step 2	**encapsulation frame-relay**	Set the encapsulation method on this interface to Frame Relay.
Step 3	**no shutdown**	Enable the configuration changes on this interface.

Verifying Your Configuration

You can verify your configuration to this point by confirming that a permanent virtual circuit (PVC) is active on the Frame Relay line, as follows:

Step 1 Wait 60 seconds after entering the **encapsulation frame-relay** command.

Step 2 From privileged EXEC command mode, enter the **show frame-relay pvc** command. You should see output similar to the following:

```
Router# show frame-relay pvc

PVC Statistics for interface Serial0 (Frame Relay DTE)

DLCI = 17, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
Serial0.1

  input pkts 45            output pkts 52           in bytes 7764
  out bytes 9958          dropped pkts 0          in FECN pkts 0
  in BECN pkts 0          out FECN pkts 0        out BECN pkts 0
  in DE pkts 0              out DE pkts 0
  pvc create time 00:30:59, last time pvc status changed 00:19:21
```

Step 3 Confirm that the “PVC STATUS=ACTIVE” message appears in the command output, as shown in the example.

Step 4 Record the number shown in the “DLCI=” message. (In this example, the number is “17.”) You use this number to finish configuring the Frame Relay interface.

Step 5 If there is no output after you enter the command, use the **show interface serial0** command to determine whether the serial interface is active. An example of this command is in the next section, "Configuring the Point-to-Point Frame Relay Connection." The first line of the command output should be as follows:

```
Serial0 is up, line protocol is up
```

If the first line of the command output is "Serial0 is up, line protocol is down," you should confirm that the Local Management Interface (LMI) type for the Frame Relay switch is correct by checking for the "LMI type is CISCO" message in the same command output.

Step 6 To continue configuration, reenter global configuration mode.

Configuring the Point-to-Point Frame Relay Connection

Follow these steps to configure the Frame Relay interface, which connects your router to the central-site router over the wide-area network.

	Command	Task
Step 1	**interface Serial0.1 point-to-point**	Enter configuration mode for the serial subinterface, and specify this interface as a point-to-point connection.
Step 2	**ip address** *192.168.39.40 255.255.255.0*	Configure this interface with an IP address and a subnet mask.
Step 3	**ipx network** *987*	Enable IPX routing on this interface.
Step 4	**frame-relay interface-dlci** *17*	Assign a data link connection identifier (DLCI) to the Frame Relay subinterface. If you are unsure of the DLCI, use the number that you recorded in Step 4 of the "Verifying Your Configuration" section on page 7-5.

	Command	Task
Step 5	**snapshot client** *5 60*	Enable snapshot routing. Because your router is dialing into a central-site router, it is considered the client router. The first number is the amount of "active time" (in minutes) during which routing updates are exchanged between your router and the central-site router. The second number is the amount of "quiet time" (in minutes) during which routing entries are frozen and remain unchanged.
Step 6	**no shutdown**	Enable the interface and the configuration changes that you have just made on the interface.
Step 7	**exit**	Exit configuration mode for this interface.

Verifying Your Configuration

You can verify your configuration to this point by

- Confirming That the Line Is Up
- Confirming That the Frame Relay Maps are Active
- Confirming Connectivity to the Central-Site Router

Confirming That the Line Is Up

To verify that the line is up, perform the following steps:

Step 1 From the privileged EXEC command mode, enter the **show interface serial0** command. You should see output similar to the following:

```
Router# show interface serial0

Serial0 is up, line protocol is up
  Hardware is QUICC Serial
__MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load
1/255
  Encapsulation FRAME-RELAY, loopback not set, keepalive set (10 sec)
  LMI enq sent  163, LMI stat recvd 136, LMI upd recvd 0, DTE LMI up
```

```
  LMI enq recvd 39, LMI stat sent  0, LMI upd sent  0
  LMI DLCI 1023  LMI type is CISCO  frame relay DTE
  Broadcast queue 0/64, broadcasts sent/dropped 27/0, interface
broadcasts 28
  Last input 00:00:01, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/64/0 (size/threshold/drops)
     Conversations  0/1 (active/max active)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1813 packets input, 109641 bytes, 0 no buffer
     Received 1576 broadcasts, 0 runts, 0 giants
     13 input errors, 0 CRC, 13 frame, 0 overrun, 0 ignored, 0 abort
     1848 packets output, 117260 bytes, 0 underruns
     0 output errors, 0 collisions, 32 interface resets
     0 output buffer failures, 0 output buffers swapped out
     29 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Step 2 Confirm that the following messages appear in the command output:

- "Serial0 is up, line protocol is up"—The Frame Relay connection is active.
- "LMI enq sent 163, LMI stat recvd 136"—The connection is sending and receiving data. The number shown in your output will probably be different.
- "LMI type is CISCO"—The LMI type is configured correctly for the router.

Step 3 If all the message do not appear in the command output, take the following steps:

a. Confirm with the Frame Relay service provider that the LMI setting is correct for your line.

b. Confirm that keepalives are set and that the router is receiving LMI updates.

Step 4 To continue configuration, reenter global configuration mode.

Confirming That the Frame Relay Maps are Active

You can verify that the frame relay maps are active by performing the following steps:

Step 1 From the privileged EXEC command mode, enter the **show frame-relay map** command. You should see output similar to the following:

```
Router# show frame-relay map
Serial0.1 (up): point-to-point dlci, dlci 17(0x11,0x410), broadcast,
          status defined, active
```

Step 2 Confirm that the "status defined, active" message appears for each serial subinterface, as shown in the example.

Step 3 If the message does not appear, proceed as follows:

a. Confirm that the central-site router is connected and configured.

b. Check with the Frame Relay carrier to verify that the line is operating correctly.

Step 4 To continue configuration, reenter global configuration mode.

Confirming Connectivity to the Central-Site Router

You can verify connectivity to the central site router by performing the following steps:

Step 1 From the privileged EXEC command mode, enter the **ping** command, followed by the IP address of the central-site router. You should see output similar to the following:

```
Router# ping 192.168.38.40

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 192.168.38.40, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32
ms
Router#
```

Step 2 Note the percentage in the "Success rate" line, as shown in the example. If the success rate is 60 percent or greater, this verification step is successful.

Step 3 To continue configuration, reenter global configuration mode.

Configuring Routing Parameters

Follow these steps to configure the Frame Relay interface for Enhanced Interior Gateway Routing Protocol (EIGRP) routing.

	Command	Task
Step 1	**router eigrp** *202*	Configure the IP EIGRP routing process.
Step 2	**network** *172.16.0.0*	To specify a list of networks for the EIGRP routing process, enter the IP address of the directly connected network.
Step 3	**ip classless**	Configure the router to forward packets addressed to a subnet of a network with no network default route.
Step 4	**exit**	Exit router configuration mode.

Configuring Command-Line Access to the Router

Follow these steps to configure parameters that control access to the router.

	Command	Task
Step 1	**line console** *0*	Specify the console terminal line.
Step 2	**exec-timeout** *5*	Set the interval in minutes that the EXEC command interpreter waits until user input is detected.
Step 3	**line vty** *0 4*	Specify a virtual terminal for remote console access.
Step 4	**password** *<lineaccess>*	Specify a password on the line.

	Command	Task
Step 5	**login**	Enable password checking at terminal session login.
Step 6	**end**	Exit configuration mode.

Frame Relay with an Internal DSU/CSU

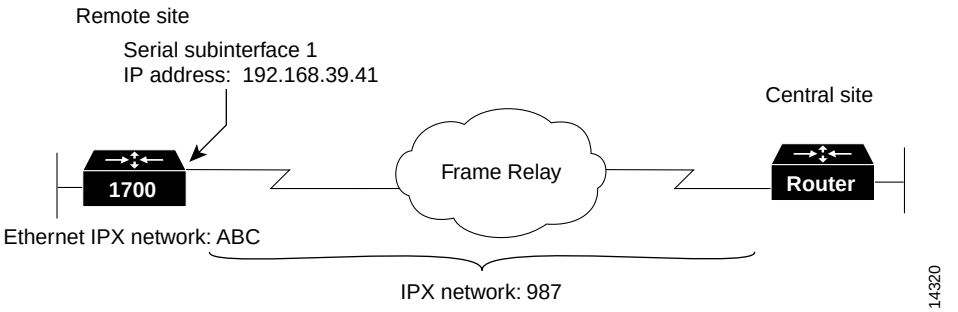
This section tells how to configure the Cisco router with an internal data service unit/channel service unit (DSU/CSU) for Frame Relay. In addition to the assumptions described in the "Before You Begin" section of this chapter, this configuration assumes that the internal DSU/CSU is a switched 56-kbps interface.

These are the major tasks in configuring your router:

- Configuring Global Parameters
- Configuring Security
- Configuring the Fast Ethernet Interface
- Configuring the Frame Relay Interface
- Configuring the Frame Relay Subinterface
- Configuring Routing Parameters
- Configuring Command-Line Access to the Router

Figure 7-2 shows the configuration example used in this section.

Figure 7-2 Configuration Example—Frame Relay Internal DSU/CSU



Configuring Global Parameters

Follow these steps to configure the router for global parameters.

	Command	Task
Step 1	**configure terminal**	Enter configuration mode.
Step 2	**service timestamps debug datetime msec**	Configure the router to show the date and time of all debug messages. This command is optional, but it is recommended if you use debug commands to troubleshoot your configuration.
Step 3	**service timestamps log datetime msec**	Configure the router to show the date and time of all log messages. This command is optional, but it is recommended if you use the verification steps described in this guide. This feature is enabled for all the command output examples shown in this guide.
Step 4	**ipx routing** *0060.834f.66dd*	Enable IPX routing, and configure the router with an IPX address.

Configuring Security

Follow these steps to configure the router with security measures.

	Command	Task
Step 1	**hostname** *Router*	Configure the router with a host name, which is used in prompts and default configuration filenames. For PPP authentication, the host name entered with this command must match the username of the central-site router.
Step 2	**enable password** <*user*>	Specify a password to prevent unauthorized access to the router.

Configuring the Fast Ethernet Interface

Follow these steps to configure the Fast Ethernet interface, which connects your router to the local network.

	Command	Task
Step 1	**interface fastethernet0**	Enter configuration mode for the Fast Ethernet interface.
Step 2	**ip address** *172.16.25.1 255.255.255.224*	Configure this interface with an IP address and a subnet mask.
Step 3	**ipx network** *ABC*	Enable IPX routing on this interface.
Step 4	**no shutdown**	Enable the interface and the configuration changes that you have just made on the interface.
Step 5	**exit**	Exit configuration mode for this interface.

Configuring the Frame Relay Interface

Follow these steps to configure the serial interface, which connects your router to the central-site router over the wide-area network.

	Command	Task
Step 1	**interface Serial0**	Enter configuration mode for the serial interface.
Step 2	**no ip address**	Disable IP routing on this interface.
Step 3	**encapsulation frame-relay**	Set the encapsulation method on this interface to Frame Relay.
Step 4	**service-module 56k clock source line**	Configure the clock source for the 56-kbps DSU/CSU module. In most applications, the DSU/CSU should be configured with the **clock source line** command. For back-to-back DSU/CSU configurations, configure one DSU/CSU with the **clock source internal** command, and configure the other with the **clock source line** command.
Step 5	**service-module 56k network type dds**	Configure this interface to transmit packets in switched dial-up mode or digital data service mode using the 56-kbps DSU/CSU module. If the clock rate has not been set correctly with the **service-module 56k clock source line** command, this command will not be accepted by the router.

Verifying Your Configuration

You can verify your configuration to this point by

- Confirming That the Line Is Up
- Confirming That the Interface Is Receiving a Line Signal

Confirming That the Line Is Up

You can verify that the line is up by performing the following steps:

Step 1 From the privileged EXEC command mode, enter the **show interface serial 0** command. You should see command output similar to the following:

```
Router# show interface serial0
Serial0 is up, line protocol is up
  Hardware is QUICC Serial
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load
1/255
  Encapsulation FRAME-RELAY, loopback not set, keepalive set (10 sec)
  LMI enq sent  163, LMI stat recvd 136, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 39, LMI stat sent  0, LMI upd sent  0
  LMI DLCI 1023  LMI type is CISCO  frame relay DTE
  Broadcast queue 0/64, broadcasts sent/dropped 27/0, interface
broadcasts 28
  Last input 00:00:01, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/64/0 (size/threshold/drops)
     Conversations  0/1 (active/max active)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1813 packets input, 109641 bytes, 0 no buffer
     Received 1576 broadcasts, 0 runts, 0 giants
     13 input errors, 0 CRC, 13 frame, 0 overrun, 0 ignored, 0 abort
     1848 packets output, 117260 bytes, 0 underruns
     0 output errors, 0 collisions, 32 interface resets
     0 output buffer failures, 0 output buffers swapped out
     29 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Step 2 Confirm that the “Serial0 is up, line protocol is up” message appears in the command output.

Step 3 To continue configuration, reenter global configuration mode.

Confirming That the Interface Is Receiving a Line Signal

You can verify that the interface is receiving a line signal by performing the following steps:

Step 1 From the privileged EXEC command mode, enter the **show service module serial0** command. You should see command output similar to the following:

```
Router# show service-module serial0
Module type is 4-wire Switched 56K in DDS mode,
Current line rate is 56 Kbits/sec and role is Telco side,
Last clearing of alarm counters 21:23:25
    oos/oof                :    0,
    loss of signal         :    0,
    loss of sealing current:    0,
    CSU/DSU loopback       :    0,
    loopback from remote   :    0,
    DTE loopback           :    0,
    line loopback          :    0,
```

Step 2 Confirm that the "loss of signal" message shows zero, which means that there are no problems with the interface receiving a line signal.

Step 3 To continue configuration, reenter global configuration mode.

Configuring the Frame Relay Subinterface

Follow these steps to configure the Frame Relay subinterface network addresses.

	Command	Task
Step 1	**interface Serial0.1 point-to-point**	Enter configuration mode for the serial subinterface, and specify this interface as a point-to-point connection.
Step 2	**ip address** *172.16.26.1 255.255.255.0*	Configure this interface with an IP address and a subnet mask.
Step 3	**ipx network** *987*	Enable IPX routing on this interface.
Step 4	**frame-relay interface-dlci** *17*	Assign a DLCI to the Frame Relay subinterface.

	Command	Task
Step 5	**ip address** *192.168.38.41 255.255.255.0*	Configure this interface with an IP address and a subnet mask.
Step 6	**ipx network** *456*	Enable IPX routing on this interface.
Step 7	**snapshot client** *5 60*	Enable snapshot routing. Because your router is dialing into a central-site router, it is considered the client router. The first number is the amount of "active time" (in minutes) during which routing updates are exchanged between your router and the central-site router. The second number is the amount of "quiet time" (in minutes) during which routing entries are frozen and remain unchanged.
Step 8	**frame-relay interface-dlci** *17*	Assign a DLCI to the Frame Relay subinterface.
Step 9	**no shutdown**	Enable the interface and the configuration changes that you have just made on the interface.
Step 10	**exit**	Exit configuration mode for the serial interface.

Configuring Routing Parameters

Follow these steps to configure the Frame Relay interface for EIGRP routing.

	Command	Task
Step 1	**router eigrp** *202*	Configure the IP EIGRP routing process.
Step 2	**network** *172.16.0.0*	To specify a list of networks for the EIGRP routing process, enter the IP address of the directly connected network.

	Command	Task
Step 3	**ip classless**	Configure the router to forward packets addressed to a subnet of a network with no network default route.
Step 4	**exit**	Exit router configuration mode.

Configuring Command-Line Access to the Router

Follow these steps to configure parameters that control access to the router.

	Command	Task
Step 1	**line console** *0*	Specify the console terminal line.
Step 2	**exec-timeout** *5*	Set the interval (in minutes) that the EXEC command interpreter waits until user input is detected.
Step 3	**line vty** *0 4*	Specify a virtual terminal for remote console access.
Step 4	**password** *<lineaccess>*	Specify a password on the line.
Step 5	**login**	Enable password checking at terminal session login.
Step 6	**end**	Exit configuration mode.

ISDN as the Backup WAN Connection

This section tells how to configure ISDN to operate as a secondary, or backup, WAN connection. With ISDN as a backup WAN connection, the router can continue to operate if the main WAN connection is down. This configuration is typically used on an ISDN WAN interface card that is installed in a Cisco router. The router onboard WAN port is the primary, or main, WAN connection, and the card WAN port is the secondary connection.

In addition to the assumptions listed in the "Before You Begin" section of this chapter, the configuration is based on the following assumptions:

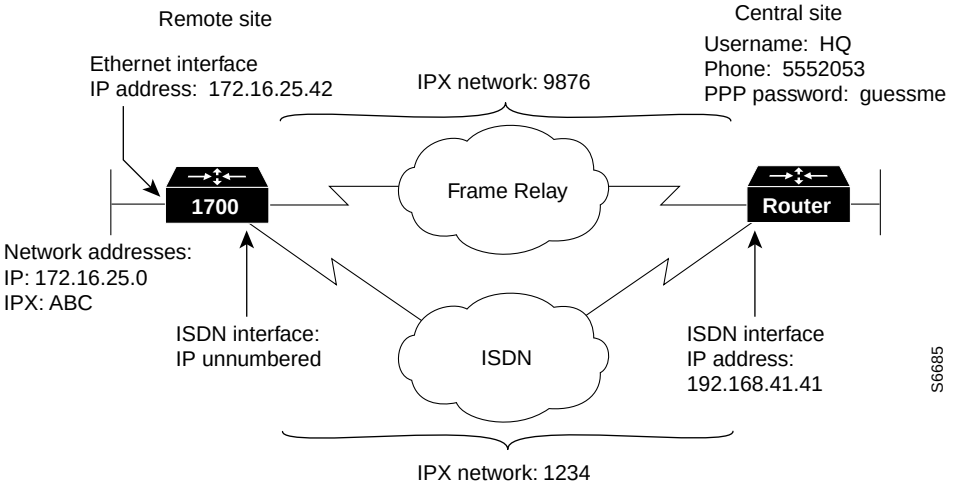
- Frame Relay is used as the primary WAN connection to the central site.
- The ISDN line is used as the secondary WAN connection to the central site.

These are the major tasks in configuring your router:

- Configuring Global Parameters
- Configuring Security
- Configuring the Fast Ethernet Interface
- Configuring the Frame Relay Interface
- Configuring the ISDN Interface
- Configuring Protocols and Dialing Behavior
- Configuring Command-Line Access to the Router

Figure 7-3 shows the configuration example used in this section.

Figure 7-3 Configuration Example—ISDN as Backup Connection



Configuring Global Parameters

Follow these steps to configure the router for some global parameters.

	Command	Task
Step 1	**configure terminal**	Enter configuration mode.
Step 2	**service timestamps debug datetime msec**	Configure the router to show the date and time of all debug messages. This command is optional, but it is recommended if you use debug commands to troubleshoot your configuration.
Step 3	**service timestamps log datetime msec**	Configure the router to show the date and time of all log messages. This command is optional, but it is recommended if you use the verification steps described in this guide. This feature is enabled for all the command output examples shown in this guide.
Step 4	**ipx routing** *0060.834f.66dd*	Configure the router with its IPX address.

	Command	Task
Step 5	**isdn switch-type** *basic-ni*	Configure the type of central office switch being used on the ISDN interface. Use the keyword that matches the ISDN switch type that you are using: • **basic-1tr6**—German 1TR6 ISDN switches • **basic-5ess**—Basic rate 5ESS switches • **basic-dms100**—NT DMS-100 basic rate switches • **basic-net3**—NET3 ISDN switches • **basic-ni**—National ISDN-1 switches • **basic-nwnet3**—Norway NET3 switches (phase 1) • **basic-nznet3**—New Zealand NET3 switches • **basic-ts013**—Australian TS013 switches • **ntt**—Japanese NTT ISDN switches • **vn2**—French VN2 ISDN switches • **vn3**—French VN3 ISDN switches

Configuring Security

Follow these steps to configure the router with security measures.

	Command	Task
Step 1	**hostname** *Router*	Configure the router with a host name, which is used in prompts and default configuration filenames. For PPP authentication, the host name entered with this command must match the username of the central-site router.
Step 2	**enable password** <*user*>	Specify a password to prevent unauthorized access to the router.
Step 3	**username** *HQ* **password** <*guessme*>	Specify the password used during caller identification and Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) authentication. For CHAP and PAP authentication, the username entered with this command must match the host name of the central-site router.

Configuring the Fast Ethernet Interface

Follow these steps to configure the Fast Ethernet interface, which connects your router to the local network.

	Command	Task
Step 1	**interface fastethernet0**	Enter configuration mode for the Fast Ethernet interface.
Step 2	**ip address** *172.16.25.1 255.255.255.0*	Configure this interface with an IP address and a subnet mask.
Step 3	**ipx network** *ABC*	Configure the Fast Ethernet interface IPX network number.

	Command	Task
Step 4	**no shutdown**	Enable the interface and the configuration changes that you have just made on the interface.
Step 5	**exit**	Exit configuration mode for the this interface.

Configuring the Frame Relay Interface

Follow these steps to configure the Frame Relay interface, which connects your router to the central-site router over the wide-area network.

	Command	Task
Step 1	**interface Serial0**	Enter configuration mode for the serial interface.
Step 2	**encapsulation frame-relay**	Set the encapsulation method on this interface to Frame Relay.
Step 3	**interface Serial0.1 point-to-point**	Enter configuration mode for the serial subinterface and specify this interface as a point-to-point connection.
Step 4	**backup interface BRI0**	Configure the BRI interface to act as a backup line for this interface.
Step 5	**backup delay** *10 10*	Define when the ISDN line is used as a backup for this interface: • The first number is the amount of time (in seconds) that the Frame Relay line is down before the ISDN line comes up as the backup line. • The second number is amount of time (in seconds) after the Frame Relay line comes back up until the ISDN line goes down.
Step 6	**ip address** *172.16.26.1 255.255.255.0*	Configure this interface with an IP address.
Step 7	**ipx network** *9876*	Enable IPX routing on this interface.

	Command	Task
Step 8	**frame-relay interface-dlci** *17*	Assign a (DLCI) to the Frame Relay subinterface.
Step 9	**no shutdown**	Enable the interface and the configuration changes that you have just made on the interface.
Step 10	**exit**	Exit configuration mode for this interface.

Configuring the ISDN Interface

Follow these steps to configure the ISDN line to act as a backup connection in the event of failure of the Frame Relay connection.

	Command	Task
Step 1	**interface BRI0**	Enter configuration mode for the ISDN interface.
Step 2	**isdn spid1** *555987601*	Enter the service profile identifier (SPID) number assigned by the ISDN service provider to the B1 channel. This step is required only when the service provider has assigned a SPID to your ISDN line. Not all ISDN lines have SPIDs.
Step 3	**isdn spid2** *555987602*	Define the SPID number assigned by the ISDN service provider to the B2 channel. This step is required only when the service provider has assigned a SPID to your ISDN line. Not all ISDN lines have SPIDs.
Step 4	**ip unnumbered fastethernet0**	Enable IP routing on this interface without assigning an IP address.
Step 5	**ipx network** *1234*	Define the IPX network number for this interface.
Step 6	**encapsulation ppp**	Set the encapsulation method on this interface to PPP.

	Command	Task
Step 7	**dialer string** *5552053*	Specify the telephone number that this interface dials to connect to the central-site router. This command is used when the interface is connecting to only a single remote site.
Step 8	**dialer-group** ***1***	Assign this interface to a dialer group.
Step 9	**ppp authentication chap pap**	Enable CHAP and PAP authentication on this interface. CHAP authentication is attempted first. If the central-site router does not support CHAP, then PAP is used for authentication.
Step 10	**ppp multilink**	Enable multilink PPP on this interface.
Step 11	**no shutdown**	Enable the interface and the configuration changes that you have just made on the interface.
Step 12	**exit**	Exit configuration mode for this interface.

Verifying Your Configuration

You can verify your configuration by confirming connectivity to the central-site router, as follows:

Step 1 From the privileged EXEC command mode, enter the **ping** command, followed by the IP address of the central-site route to have the router dial the remote router. You should see command output similar to the following:

```
Router# ping 192.168.37.40

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.37.40, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 40/43/48 ms
Router#
*Mar  1 03:37:46.526: %LINK-3-UPDOWN: Interface BRI0:1, changed state
to up
*Mar  1 03:37:46.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface
BRI0:1, changed state to up
*Mar  1 03:37:46.939: %LINK-3-UPDOWN: Interface Virtual-Access1,
changed state to up
```

```
*Mar  1 03:37:47.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access1, changed state to up
 *Mar  1 03:35:57.217: %ISDN-6-CONNECT: Interface BRI0:1 is now
connected to 5552053 HQ
```

Step 2 Wait for the "ISDN-6-CONNECT" message.

Step 3 Enter the **ping** command, followed by the IP address of the central-site router, a second time:

```
Router# ping 192.168.37.40

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.37.40, timeout is 2 seconds:
.!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/43/48
ms
Router#
*Mar  1 03:37:46.526: %LINK-3-UPDOWN: Interface BRI0:1, changed state
to up
*Mar  1 03:37:46.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface
BRI0:1, changed state to up
*Mar  1 03:37:46.939: %LINK-3-UPDOWN: Interface Virtual-Access1,
changed state to up
*Mar  1 03:37:47.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access1, changed state to up
 *Mar  1 03:35:57.217: %ISDN-6-CONNECT: Interface BRI0:1 is now
connected to 5552053 HQ
```

Step 4 If the success rate is 100 percent, this verification step is successful.

Step 5 If the success rate is less than 60 percent, take the following steps:

a. Use the **show frame-relay pvc** command to confirm that the DLCI for the Frame Relay interface is active.

b. Use the **show interface serial0** command to confirm that the "Serial0 is up, line protocol is up" message is displayed in the command output.

Step 6 To continue configuration, reenter global configuration mode.

Configuring Protocols and Dialing Behavior

Follow these steps to configure how and when the ISDN line connects to the central-site router.

	Command	Task
Step 1	**router eigrp** *202*	Configure the IP (EIGRP) routing process.
Step 2	**network** *172.16.0.0*	To specify a list of networks for the EIGRP routing process, enter the IP address of the directly connected network.
Step 3	**ip classless**	Specify that the router does not forward packets that are destined for a subnet of a network that has no network default route.
Step 4	**dialer-list** *1* **protocol ip permit**	Specify an access list both by list number and by protocol (IP) to define the packets of interest that can trigger a called to the destination.
Step 5	**dialer-list** *1* **protocol ipx permit**	Specify an access list both by list number and by protocol (IPX) to define the packets of interest that can trigger a called to the destination.
Step 6	**exit**	Exit router configuration mode.

Configuring Command-Line Access to the Router

Follow these steps to configure parameters that control access to the router.

	Command	Task
Step 1	**line console** *0*	Specify the console terminal line.
Step 2	**exec-timeout** *5*	Set the interval that the EXEC command interpreter waits until user input is detected.
Step 3	**line vty** *0 4*	Specify a virtual terminal for remote console access.
Step 4	**password** *<lineaccess>*	Specify a password on the line.
Step 5	**login**	Enable password checking at terminal session login.
Step 6	**end**	Exit configuration mode.

Verifying Your Configuration

To verify your router configuration to this point, confirm that the ISDN connects dynamically to the remote site when the Frame Relay connection is disconnected. Follow these steps:

Step 1 Remove the cable that connects the router to the Frame Relay services, or otherwise force the DLCI(s) to become inactive. This action brings the line protocol down.

Step 2 When the router generates routing updates, the ISDN line should begin dialing. If the ISDN line does not dial, use the **ping** command as described in the "Configuring the ISDN Interface" section.

Step 3 Reconnect the cable that connects the router to the Frame Relay services, or force the DLCI(s) to become active. The ISDN line should disconnect dynamically.

Troubleshooting Problems with ISDN as Frame Relay Backup Line

If you are having problems, follow some or all of these steps:

Step 1 Confirm that you used the **broadcast** keyword in the **dialer map** command. This keyword causes dialing to occur with a flash routing update. If you do not use the **broadcast** keyword, routing updates do not trigger dialing on the ISDN line.

Step 2 If you want to use the ISDN line even when the Frame Relay line is connected, use dialer profiles. Otherwise, the ISDN line operates in backup mode only.

Step 3 If you are having problems, you can use some or all of the following debug commands:

- **debug dialer events**
- **debug isdn events**
- **debug isdn q931**
- **debug isdn q921**
- **debug ppp negotiation**

- **debug ppp authentication**
- **debug ppp multilink events**

Caution If you are not familiar with Cisco IOS debug commands, you should read the "Using Debug Commands" section in the "Introduction to Router Configuration" chapter before attempting any debugging.

ISDN as a Backup Connection with Dialer Profiles

This section describes how to configure ISDN to operate as a secondary, or backup, WAN connection by using dialer profiles to connect to multiple central-site routers.

In addition to the assumptions listed in the "Before You Begin" section at the beginning of this chapter, this configuration is based on the following additional assumptions:

- The Frame Relay service provides end-to-end status of the Frame Relay connection.

  This means that if the router primary serial WAN connection (in this example, Frame Relay) goes down, the Frame Relay switch sends LMI updates to the central-site router, indicating that the line has gone down.
- Your router connects to two different central-site routers.

These are the major tasks in configuring your router:

- Configuring Global Parameters
- Configuring Security
- Configuring the Fast Ethernet Interface
- Configuring the Serial Interface
- Configuring the Primary Connection to the First Central-Site Router
- Configuring the Primary Connection to the Second Central-Site Router
- Configuring the ISDN Interface
- Configuring the Backup Connection to the First Central-Site Router
- Configuring the Backup Connection to the Second Central-Site Router
- Configuring Routing Protocols
- Configuring Command-Line Access to the Router

Configuring Global Parameters

Follow these steps to configure the router for global parameters.

	Command	Task
Step 1	**configure terminal**	Enter configuration mode.
Step 2	**service timestamps debug datetime msec**	Configure the router to show the date and time of all debug messages. This command is optional, but it is recommended if you use debug commands to troubleshoot your configuration.
Step 3	**service timestamps log datetime msec**	Configure the router to show the date and time of all log messages. This command is optional, but it is recommended if you use the verification steps described in this guide. This feature is enabled for all the command output examples shown in this guide.

	Command	Task
Step 4	**isdn switch-type** *basic-ni*	Configure the type of central office switch being used on the ISDN interface. Use the keyword that matches the ISDN switch type that you are using: • **basic-1tr6**—German 1TR6 ISDN switches • **basic-5ess**—Basic rate 5ESS switches • **basic-dms100**—NT DMS-100 basic rate switches • **basic-net3**—NET3 ISDN switches • **basic-ni**—National ISDN-1 switches • **basic-nwnet3**—Norway NET3 switches (phase 1) • **basic-nznet3**—New Zealand NET3 switches • **basic-ts013**—Australian TS013 switches • **ntt**—Japanese NTT ISDN switches • **vn2**—French VN2 ISDN switches • **vn3**—French VN3 ISDN switches

Configuring Security

Follow these steps to configure the router with security measures.

	Command	Task
Step 1	**hostname** *Router*	Configure the router with a host name, which is used in prompts and default configuration filenames. For PPP authentication, the host name entered with this command must match the username of the central-site router.
Step 2	**enable password** <*user*>	Specify a password to prevent unauthorized access to the router.
Step 3	**username** *HQ1* **password** <*guessme1*>	Specify the password used during caller identification and CHAP and PAP authentication. This password applies only to one of the central-site routers. For security reasons, a different password should be used for each remote location that the router dials on the backup ISDN line. For PPP authentication, the username entered with this command must match the host name of the central-site router.
Step 4	**username** *HQ2* **password** <*guessme2*>	Specify the password used during caller identification and CHAP and PAP authentication. This password applies only to one of the central-site routers. For security reasons, a different password should be used for each remote location that the router dials on the backup ISDN line. For PPP authentication, the username entered with this command must match the host name of the central-site router.

Configuring the Fast Ethernet Interface

Follow these steps to configure the Fast Ethernet interface, which connects your router to the local network.

	Command	Task
Step 1	**interface fastethernet0**	Enter configuration mode for this interface.
Step 2	**ip address** *172.16.20.1 255.255.255.0*	Configure this interface with an Ethernet address.
Step 3	**no ip route-cache**	Disable fast switching and autonomous switching on this interface.
Step 4	**ip mroute-cache**	Enable IP multicast fast switching on this interface.
Step 5	**no shutdown**	Enable the configuration changes for this interface.
Step 6	**exit**	Exit configuration mode for this interface.

Configuring the Serial Interface

Follow these steps to configure the serial interface, which connects your router to the central-site router over the wide-area network.

	Command	Task
Step 1	**interface serial0**	Enter configuration mode for this interface.
Step 2	**no ip address**	Disable IP processing for this interface.
Step 3	**encapsulation frame-relay**	Configure this interface for Frame Relay encapsulation.
Step 4	**no shutdown**	Enable the configuration changes for this interface.
Step 5	**exit**	Exit configuration mode for this interface.

Configuring the Primary Connection to the First Central-Site Router

Follow these steps to configure a Frame Relay connection to a central-site router.

	Command	Task
Step 1	**interface serial0.1 point-to-point**	Create a subinterface, and enter configuration mode for the interface.
Step 2	**backup delay** *10 10*	Define when the ISDN line is used as a backup for this interface: • The first number is the amount of time (in seconds) that the Frame Relay line is down before the ISDN line comes up as the backup line. • The second number is amount of time (in seconds) after the Frame Relay line comes back up until the ISDN line goes down.
Step 3	**backup interface Dialer1**	Configure the BRI interface to act as a dial backup line for this subinterface.
Step 4	**ip address** *172.16.30.40 255.255.255.0*	Configure this subinterface with an IP address.
Step 5	**ipx network** *AABB*	Configure this subinterface with an IPX network address.
Step 6	**frame-relay interface-dlci** *17*	Assign a DLCI to this subinterface.
Step 7	**no shutdown**	Enable the configuration changes for this subinterface.
Step 8	**exit**	Exit configuration mode for this subinterface.

Configuring the Primary Connection to the Second Central-Site Router

Follow these steps to configure a Frame Relay connection to a second central-site router.

	Command	Task
Step 1	**interface serial0.2 point-to-point**	Create a subinterface, and enter configuration mode for the interface.
Step 2	**backup delay** *10 10*	Define when the ISDN line is used as a backup for this interface: • The first number is the amount of time (in seconds) that the Frame Relay line is down before the ISDN line comes up as the backup line. • The second number is amount of time (in seconds) after the Frame Relay line comes back up until the ISDN line goes down.
Step 3	**backup interface Dialer2**	Configure the BRI interface to act as a dial backup line for this subinterface.
Step 4	**ip address** *172.16.40.40 255.255.255.0*	Configure this subinterface with an IP address.
Step 5	**ipx network** *BBCC*	Configure this subinterface with an IPX network address.
Step 6	**frame-relay interface-dlci** *18*	Assign a DLCI to this subinterface.
Step 7	**no shutdown**	Enable the configuration changes for this subinterface.
Step 8	**exit**	Exit configuration mode for this subinterface.

Configuring the ISDN Interface

Follow these steps to configure the ISDN line to act as a backup connection in the event of failure of the Frame Relay connection.

	Command	Task
Step 1	**interface BRI0**	Enter configuration mode for this interface.
Step 2	**encapsulation ppp**	Configure this interface for PPP packet encapsulation.
Step 3	**dialer pool-member** *1*	Assign this interface to a dialer pool.
Step 4	**no shutdown**	Enable the configuration changes on this interface.
Step 5	**exit**	Exit configuration mode for this interface.

Configuring the Backup Connection to the First Central-Site Router

Follow these steps to configure the ISDN backup connection to one central-site router.

	Command	Task
Step 1	**interface Dialer1**	Create an ISDN dialer interface, and enter configuration mode for the interface. The number that you assign in this command must match the number you assigned with the **backup interface** command when you configured the primary connection to the first central-site router.
Step 2	**ip unnumbered fastethernet0**	Enable IP routing without assigning an IP address.
Step 3	**encapsulation ppp**	Configure this interface for PPP packet encapsulation.

	Command	Task
Step 4	**ipx network** *DCBA*	Configure this interface with an IPX network number.
Step 5	**dialer remote-name** *HQ1*	Configure the name of the central-site router that this interface dials. The name that you enter with this command should be the same name that you entered with the **username password** command in the "Configuring Security" section on page 7-32.
Step 6	**dialer string** *5551234*	Configure the number that the interface dials to connect to the central-site router.
Step 7	**dialer max-call** *1*	Specify that the router can have only one call connected to the first central-site router at any one time.
Step 8	**dialer pool** *1*	Assign this interface to a dialer pool.
Step 9	**dialer-group** *1*	Assign this interface to a dialer group.
Step 10	**ppp authentication chap pap**	Enable CHAP and PAP authentication on this interface. CHAP authentication is attempted first. If the central-site router does not support CHAP, then PAP is used for authentication.
Step 11	**no shutdown**	Enable the configuration changes for this interface.
Step 12	**exit**	Exit configuration mode for this subinterface.

Configuring the Backup Connection to the Second Central-Site Router

Follow these steps to configure the ISDN backup connection to a second central-site router.

	Command	Task
Step 1	**interface Dialer2**	Create an ISDN dialer interface, and enter configuration mode for the interface. The number that you assign in this command must match the number you assigned with the **backup interface** command when you configured the primary connection to the second central-site router.
Step 2	**ip unnumbered fastethernet0**	Enable IP routing without assigning an IP address.
Step 3	**encapsulation ppp**	Configure this interface for PPP packet encapsulation.
Step 4	**ipx network** *ABCD*	Configure this interface with an IPX network number.
Step 5	**dialer remote-name** *HQ2*	Configure the name of the central-site router that this interface dials. The name that you enter with this command should be the same name that you entered with the **username password** command in the "Configuring Security" section on page 7-32.
Step 6	**dialer string** *5551122*	Configure the number that the interface dials to connect to the central-site router.
Step 7	**dialer max-call** *1*	Specify that the router can have only one call connected to the first central-site router at any one time.
Step 8	**dialer pool** *1*	Assign this interface to a dialer pool.
Step 9	**dialer-group** *1*	Assign this interface to a dialer group.
Step 10	**ppp authentication chap pap**	Enable CHAP and PAP authentication on this interface. CHAP authentication is attempted first. If the central-site router does not support CHAP, then PAP is used for authentication.

	Command	Task
Step 11	**no shutdown**	Enable the configuration changes for this interface.
Step 12	**exit**	Exit configuration mode for this subinterface.

Configuring Routing Protocols

Follow these steps to configure the router for EIGRP routing.

	Command	Task
Step 1	**router eigrp** *1*	Configure the router for IP EIGRP routing.
Step 2	**network** *172.16.0.0*	Configure the IP network address for EIGRP routing.
Step 3	**exit**	Exit router configuration mode.

Configuring Command-Line Access to the Router

Follow these steps to configure parameters that control access to the router.

	Command	Task
Step 1	**line console** *0*	Specify the console terminal line.
Step 2	**exec-timeout** *5*	Set the interval (in minutes) that the EXEC command interpreter waits until user input is detected.
Step 3	**line vty** *0 4*	Specify a virtual terminal for remote console access.
Step 4	**password** *<lineaccess>*	Specify a password on the line.
Step 5	**login**	Enable password checking at terminal session login.
Step 6	**end**	Exit configuration mode.

ISDN as a Backup Connection with Floating Static Routes

When the router makes routing decisions, static routes normally take precedence over learned routes. If you have configured static routes, the router usually sends data over these routes before using routes that it has learned and stored in the routing table.

However, when the ISDN line is used as a backup connection and is configured with static routes, the primary WAN connection (the Frame Relay line) does not come back up when the ISDN line is used. Floating static routes enable the ISDN line to use static routes to the central-site router until the main WAN connection, the Frame Relay line, is active again.

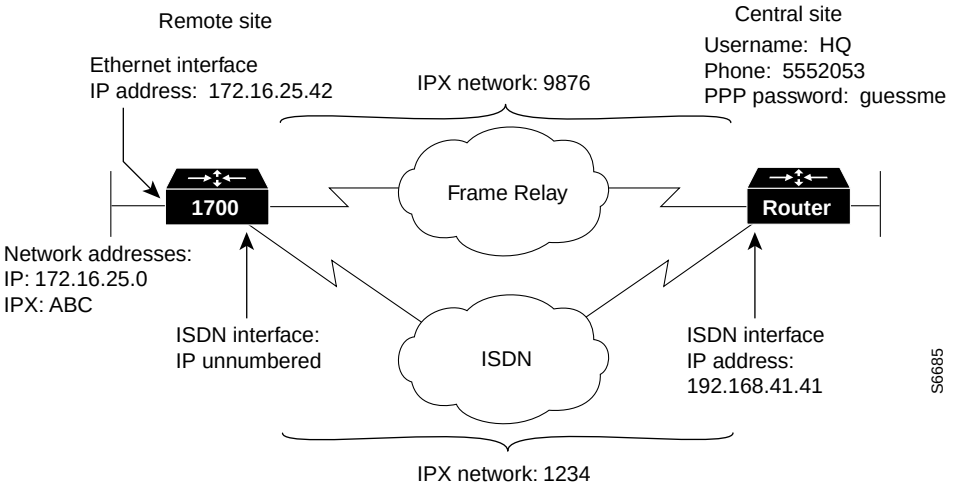
This section describes how to configure ISDN to operate as a secondary, or backup, WAN connection with floating static routes.

These are the major tasks in configuring your router:

- Configuring Global Parameters
- Configuring Security
- Configuring the Fast Ethernet Interface
- Configuring the Frame Relay Interface
- Configuring the Frame Relay Subinterface
- Configuring the ISDN Interface
- Configuring EIGRP Routing
- Configuring When the Router Dials Out
- Configuring Command-Line Access to the Router

Figure 7-4 shows the configuration example used in this section.

Figure 7-4 Configuration Example—ISDN as Backup Connection with Floating Static Routes



Assumptions

In addition to the assumptions listed in the "Before You Begin" section of this chapter, the configuration in this section is based on the following assumptions:

- Frame Relay is being used as the primary WAN connection to the central site.
- You are routing IP data.
- The ISDN line is the being used as the secondary WAN connection to the central site.

Configuring Global Parameters

Follow these steps to configure the router for some global parameters.

	Command	Task
Step 1	**configure terminal**	Enter configuration mode.
Step 2	**service timestamps debug datetime msec**	Configure the router to show the date and time of all debug messages. This command is optional, but it is recommended if you use debug commands to troubleshoot your configuration.
Step 3	**service timestamps log datetime msec**	Configure the router to show the date and time of all log messages. This command is optional, but it is recommended if you use the verification steps described in this guide. This feature is enabled for all the command output examples shown in this guide.

	Command	Task
Step 4	**isdn switch-type** *basic-ni*	Configure the type of central office switch being used on the ISDN interface. Use the keyword that matches the ISDN switch type that you are using: • **basic-1tr6**—German 1TR6 ISDN switches • **basic-5ess**—Basic rate 5ESS switches • **basic-dms100**—NT DMS-100 basic rate switches • **basic-net3**—NET3 ISDN switches • **basic-ni**—National ISDN-1 switches • **basic-nwnet3**—Norway NET3 switches (phase 1) • **basic-nznet3**—New Zealand NET3 switches • **basic-ts013**—Australian TS013 switches • **ntt**—Japanese NTT ISDN switches • **vn2**—French VN2 ISDN switches • **vn3**—French VN3 ISDN switches

Configuring Security

Follow these steps to configure the router with security measures.

	Command	Task
Step 1	**hostname** *Router*	Configure the router with a host name, which is used in prompts and default configuration filenames. For PPP authentication, the host name entered with this command must match the username of the central-site router.

	Command	Task
Step 2	**enable password** <*user*>	Specify a password to prevent unauthorized access to the router.
Step 3	**username** *HQ* **password** <*guessme*>	Specify the password used during caller identification and CHAP and PAP authentication. For CHAP and PAP authentication, the username entered with this command must match the host name of the central-site router.

Configuring the Fast Ethernet Interface

Follow these steps to configure the Fast Ethernet interface, which connects your router to the local network.

	Command	Task
Step 1	**interface fastethernet0**	Enter configuration mode for the Fast Ethernet interface.
Step 2	**ip address** *172.16.25.1 255.255.255.224*	Configure this interface with an IP address and a subnet mask.
Step 3	**no shutdown**	Enable the interface and the configuration changes that you have just made on the interface.
Step 4	**exit**	Exit configuration mode for the this interface.

Configuring the Frame Relay Interface

Follow these steps to configure parameters for the Frame Relay interface, which connects your router to the central-site router over the wide-area network.

	Command	Task
Step 1	**interface Serial0**	Enter configuration mode for the serial interface.
Step 2	**no ip address**	Disable IP routing on this interface.
Step 3	**encapsulation frame-relay**	Set the encapsulation method on this interface to Frame Relay.
Step 4	**no shutdown**	Enable the interface and the configuration changes that you have just made on the interface.
Step 5	**exit**	Exit configuration mode for this interface.

Configuring the Frame Relay Subinterface

Follow these steps to configure the Frame Relay subinterface network addresses.

	Command	Task
Step 1	**interface serial0.1 point-to-point**	Enter configuration mode for the serial subinterface, and specify this interface as a point-to-point connection.
Step 2	**ip address** *192.168.39.41 255.255.255.0*	Configure this subinterface with an IP address.
Step 3	**ipx network** *9876*	Configure this subinterface with an IPX network number.
Step 4	**frame-relay interface-dlci** *17*	Assign a DLCI to the Frame Relay subinterface. If you are unsure of the DLCI, use the number that you recorded in Step 4 of the "Verifying Your Configuration" section on page 7-28.
Step 5	**exit**	Exit configuration mode for this interface.

Configuring the ISDN Interface

Follow these steps to configure parameters for the ISDN interface, which connects your router to the central-site router if for some reason the Frame Relay connection fails.

	Command	Task
Step 1	**interface BRI0**	Enter configuration mode for the ISDN interface.
Step 2	**isdn spid1** *555987601*	Enter the SPID number assigned by the ISDN service provider to the B1 channel. This step is required only when the service provider has assigned a SPID to your ISDN line. Not all ISDN lines have SPIDs.
Step 3	**isdn spid2** *555987602*	Define the SPID number assigned by the ISDN service provider to the B2 channel. This step is required only when the service provider has assigned a SPID to your ISDN line. Not all ISDN lines have SPIDs.
Step 4	**ip unnumbered fastethernet0**	Enable IP routing on this interface without assigning an IP address.
Step 5	**encapsulation ppp**	Set the encapsulation method on this interface to PPP.
Step 6	**ipx network** *1234*	Configure this interface with an IPX network number.
Step 7	**ipx delay** *200*	Configure this interface to exchange routing information while the ISDN line is up. Routing updates do not bring up the ISDN line if it is down.
Step 8	**no ip route-cache**	Disable fast switching and autonomous switching on this interface.
Step 9	**ipx watchdog-spoof**	Set the router to respond to local server watchdog packets on behalf of a remote client (called *spoofing*).

	Command	Task
Step 10	**dialer idle-timeout** *300*	Configure the ISDN line to go down after a specified number of seconds with no network traffic.
Step 11	**dialer string** *5552053*	Configure the telephone number that this interface dials to reach the central site.
Step 12	**dialer-group** *1*	Assign this interface to a dialer group.
Step 13	**no fair-queue**	Disable weighted fair queuing for this interface.
Step 14	**ppp authentication chap pap**	Enable CHAP and PAP authentication on this interface. CHAP authentication is attempted first. If the central-site router does not support CHAP, then PAP is used for authentication.
Step 15	**ppp multilink**	Enable multilink PPP on this interface.
Step 16	**no shutdown**	Enable the interface and the configuration changes that you have just made on the interface.
Step 17	**exit**	Exit configuration mode for this interface.

Configuring EIGRP Routing

Follow these steps to configure the router for EIGRP and IP routing parameters that the router uses to connect to the central-site router.

	Command	Task
Step 1	**router eigrp** *202*	Configure the IP EIGRP routing process.
Step 2	**network** *172.16.0.0*	Specify a list of networks for the EIGRP routing process by entering the IP address of the directly connected network.
Step 3	**network** *192.168.0.0*	To specify a list of networks for the EIGRP routing process, enter the IP address of the directly connected network.

	Command	Task
Step 4	**ip classless**	Specify that the router does not forward packets that are destined for a subnet of a network that has no network default route.
Step 5	**exit**	Exit router configuration mode.

Configuring When the Router Dials Out

Follow these steps to configure access lists and static routes that determine when the ISDN line dials the central-site router.

	Command	Task
Step 1	**ip route 0.0.0.0 0.0.0.0** *192.168.41.41 150*	Establish a static IP route to the remote network.
Step 2	**ip route** *192.168.41.41 255.255.0.0* **BRI0**	Establish a static IP route on the BRI interface to the remote network.
Step 3	**access-list** *101* **deny ip any** *224.0.0.0 31.255.255.255*	Define a standard access list based on network variables.
Step 4	**access-list** *101* **permit ip any any**	Define a standard access list based on network variables.
Step 5	**access-list** *900* **deny any any all any** *457*	Define a standard access list based on network variables.
Step 6	**access-list** *900* **deny rip any rip any rip**	Define a standard access list based on network variables.
Step 7	**access-list** *900* **deny sap any sap any sap**	Define a standard access list based on network variables.
Step 8	**access-list** *900* **permit any any all any all**	Define a standard access list based on network variables.
Step 9	**ipx route** *CBA 1234.0000.0c75.c689* **floating-static**	Define a floating static IPX route to the central-site network.
Step 10	**ipx route** *CCB 1234.0000.0c75.c689* **floating-static**	Define a floating static IPX route to the central-site network.

	Command	Task
Step 11	**ipx route** *5E11 1234.0000.0c75.c689* **floating-static**	Define a floating static IPX route to the central-site network.
Step 12	**ipx sap** *4 MRKT_SERV 5E11.0000.0000.0001 452 2*	Define a static route to an IPX server on the central-site network.
Step 13	**ipx sap** *4 ENG_SERV CCB.0000.0000.0001 452 2*	Define a static route to an IPX server on the central-site network.
Step 14	**ipx sap** *4 CORP_SERV CBA.0000.0000.0001 452 2*	Define a static route to an IPX server on the central-site network.
Step 15	**dialer-list** *1* **protocol ipx list** *900*	Specify a dialer list both by list number and by protocol (IPX) to define the packets of interest that can trigger a call to the destination.
Step 16	**dialer-list** *1* **protocol ip list** *101*	Specify a dialer list both by list number and by protocol (IP) to define the packets of interest that can trigger a call to the destination.

Configuring Command-Line Access to the Router

Follow these steps to configure parameters that control access to the router.

	Command	Task
Step 1	**line console** *0*	Specify the console terminal line.
Step 2	**exec-timeout** *5*	Set the interval (in minutes) that the EXEC command interpreter waits until user input is detected.
Step 3	**line vty** *0 4*	Specify a virtual terminal for remote console access.
Step 4	**password** *<lineaccess>*	Specify a password on the line.
Step 5	**login**	Enable password checking at terminal session login.
Step 6	**end**	Exit configuration mode.

Verifying Your Configuration

Follow these steps to verify that the ISDN line is configured to back up the Frame Relay line:

Step 1 Bring the Frame Relay connection down. This clears the routing table of all routes learned from the Frame Relay interface.

Step 2 Use the **ping** command to test connectivity to any central-site router that is on the 192.168.0.0 network. This should cause the ISDN line to connect dynamically and dial the central-site router.

Step 3 Bring the Frame Relay connection back up, and confirm that the ISDN link disconnects.

Troubleshooting Floating Static Route Problems

If you are having problems or if the output that you received during the verification steps is very different from that shown in the command output examples, you can troubleshoot your router with the Cisco IOS debug commands. The debug commands provide extensive command output that is not included in this document.

Caution If you are not familiar with Cisco IOS debug commands, you should read the "Using Debug Commands" section in the "Introduction to Router Configuration" chapter before attempting any debugging.

Following are debug commands that are helpful when troubleshooting ISDN with IP and IPX routing. Follow these commands with the **ping** command to display debug output:

- **debug dialer events**
- **debug isdn events**
- **debug isdn q931**
- **debug isdn q921**
- **debug ppp negotiation**

- **debug ppp authentication**
- **debug ppp multilink events**

CHAPTER 8

Configuring Asynchronous Connections

This chapter describes how to configure the Cisco router to dial into a central-site router over a standard telephone line and provides verification steps and troubleshooting tips.

This chapter contains the following sections:

- Before You Begin
- Asynchronous Dial-Up Connection
- Asynchronous Dial-In Pool
- Troubleshooting Asynchronous Problems

Before You Begin

The configurations in this chapter are based on the following assumptions:

- Your Cisco router hardware is correctly installed in accordance with the Hardware Installation Guide for your Cisco router.
- Your Cisco router is using Point-to-Point Protocol (PPP).

Before you begin configuration, be aware of the following:

- You need to enter the commands in the order shown in the task tables.
- The values shown in italic are examples. For the values shown, you should instead enter values appropriate for your network.

- You should be familiar with Cisco IOS software and its conventions.

Note To use the verification steps described in this chapter, you must be familiar with Cisco IOS commands and command modes. When you use the verification steps, you need to change to different command modes. If you are not familiar with command modes, see the "Understanding Command Modes" section in the "Introduction to Router Configuration" chapter.

Asynchronous Dial-Up Connection

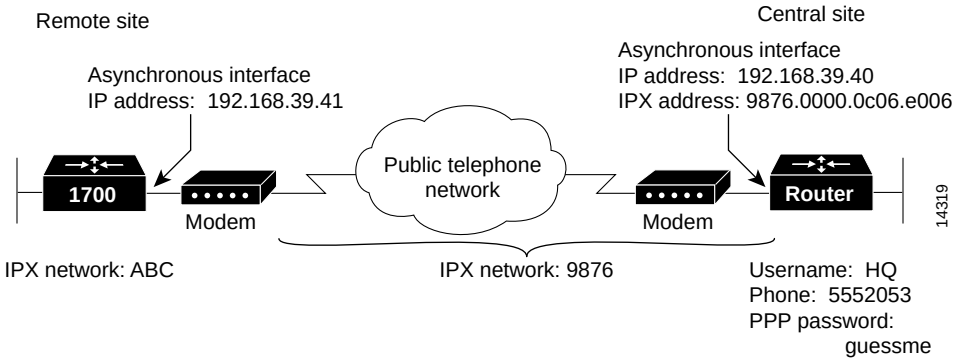
In this configuration, a modem is attached to the router serial port. The modem dials into the central-site router over a standard telephone line, which is an asynchronous connection. The Cisco router is dialing into a central-site router.

These are the major tasks in configuring your router for an asynchronous dial-up connection:

- Configuring Global Parameters
- Configuring Security
- Configuring the Fast Ethernet Interface
- Configuring the Asynchronous Interface
- Configuring When the Router Dials
- Configuring Command-Line Access to the Router

Figure 8-1 shows the configuration example used in this section.

Figure 8-1 Configuration Example—Asynchronous Dial-Up Connection



Configuring Global Parameters

Follow these steps to configure global parameters.

	Command	Task
Step 1	**configure terminal**	Enter configuration mode.
Step 2	**service timestamps debug datetime msec**	Configure the router to show the date and time of all debug messages. This command is optional, but it is recommended if you use debug commands to troubleshoot your configuration.
Step 3	**service timestamps log datetime msec**	Configure the router to show the date and time of all log messages. This command is optional, but it is recommended if you use the verification steps described in this guide. This feature is enabled for all the command output examples shown in this guide.

	Command	Task
Step 4	**ipx routing** *0060.834f.66dd*	Enable Internetwork Packet Exchange (IPX) routing and configure the router with an IPX address.
Step 5	**chat-script** *dialout "atdt\t" timeout 60 connect\c*	Create a script that causes the modem connected to the router to place a call to the central site.

Configuring Security

Follow these steps to configure the router with security measures.

	Command	Task
Step 1	**enable password** <*user*>	Specify a password to prevent unauthorized access to the router.
Step 2	**hostname** *Router*	Configure the router with a host name, which is used in prompts and default configuration file names. For PPP authentication, the host name entered with this command must match the username of the central-site router.
Step 3	**username** *HQ* **password** <*guessme*>	Specify the password used during caller identification and Challenge Handshake Authorization Protocol (CHAP) and Password Authorization Protocol (PAP) authentication. For CHAP and PAP authentication, the username entered with this command must match the host name of the central-site router.

Configuring the Fast Ethernet Interface

Follow these steps to configure the Fast Ethernet interface, which connects your router to the local network.

	Command	Task
Step 1	**interface fastethernet0**	Enter configuration mode for the Fast Ethernet interface.
Step 2	**ip address** *172.16.25.42 255.255.255.224*	Configure this interface with an IP address and a subnet mask.
Step 3	**ipx network** *ABC*	Configure an IPX network address for this interface.
Step 4	**no shutdown**	Enable the interface and the configuration changes that you have just made on the interface.
Step 5	**exit**	Exit configuration mode for the interface.

Configuring the Asynchronous Interface

Follow these steps to configure the asynchronous interface, which connects your router to the central-site router over the wide-area network.

	Command	Task
Step 1	**interface Serial0**	Enter configuration mode for the serial interface.
Step 2	**physical-layer async**	Specify the mode of this slow-speed serial interface as asynchronous.
Step 3	**async mode dedicated**	Configure the asynchronous line for data traffic, rather than for EXEC command line sessions.
Step 4	**ip address** *192.168.39.41 255.255.255.0*	Configure this interface with an IP address and a subnet mask.
Step 5	**ipx network** *9876*	Enable IPX routing on this interface.

	Command	Task
Step 6	**dialer in-band**	Specify that dial-on-demand routing (DDR) is supported on this interface.
Step 7	**ipx route** *1234 9876.0000.0c06.ecc6*	Configure a static route to the central-site device.
Step 8	**snapshot client** *5 60*	Enable snapshot routing. Because your router is dialing into a central-site router, it is considered the client router. The first number is the amount of "active time" (in minutes) during which routing updates are exchanged between your router and the central-site router. The second number is the amount of "quiet time" (in minutes) during which routing entries are frozen and remain unchanged.
Step 9	**dialer-group** *1*	Assign the dialer interface to a dialer group.
Step 10	**encapsulation ppp**	Set the encapsulation method on this interface to PPP.
Step 11	**ppp authentication chap pap callin**	Enable CHAP or PAP authentication on this interface. CHAP authentication is attempted first.
Step 12	**no shutdown**	Enable the interface and the configuration changes that you have just made on the interface.
Step 13	**exit**	Exit configuration mode for this interface.
Step 14	**line 1**	Enter configuration mode for the serial0 interface.
Step 15	**speed** *19200*	Configure the baud rate for the asynchronous line.
Step 16	**parity** *n*	Configure parity on the asynchronous line.
Step 17	**datab** *8*	Configure data bits on the asynchronous line.

	Command	Task
Step 18	**stopb** *1*	Configure stop bits on the asynchronous line.
Step 19	**exit**	Exit line configuration mode.

Verifying Your Configuration

You can verify your configuration to this point by

- Confirming Connectivity to the Central-Site Router
- Confirming the Serial Interface Status
- Confirming the Asynchronous Line Configuration

Confirming Connectivity to the Central-Site Router

Follow these steps to verify connectivity to the central-site router:

Step 1 From the privileged EXEC command mode, enter the **ping** command, followed by the IP address of the central-site router. Yous should see command output similar to the following.

Note The modem might need time to synchronize with the central-site modem. You might have to enter the **ping** command several times before you get a response.

```
Router# ping 192.168.37.40

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 192.168.37.40, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 40/43/48 ms
Router#
*Mar  1 03:37:46.526: %LINK-3-UPDOWN: Interface BRI0:1, changed state
to up
*Mar  1 03:37:46.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface
BRI0:1, changed state to up
*Mar  1 03:37:46.939: %LINK-3-UPDOWN: Interface Virtual-Access1,
changed state to up
*Mar  1 03:37:47.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access1, changed state to up
 *Mar  1 03:35:57.217: %ISDN-6-CONNECT: Interface BRI0:1 is now
connected to 5552053 HQ
```

Step 2 Note the percentage in the “Success rate” line. A success rate of 60 percent or greater means that your router is successfully transferring data to the central-site router.

Step 3 To continue configuration, reenter global configuration mode.

Confirming the Serial Interface Status

Follow these steps to confirm the status of the serial interface:

Step 1 From the privileged EXEC command mode, enter the **show interface serial0** command. You should see command output similar to the following:

```
Router# show interface serial0
Serial0 is up, line protocol is up
  Hardware is PQUICC Serial in async mode (TTY1)
  Internet address is 12.0.0.2/8
  MTU 1500 bytes, BW 19 Kbit, DLY 100000 usec, rely 255/255, load
1/255
  Encapsulation PPP, loopback not set, keepalive not set
  DTR is pulsed for 5 seconds on reset
  LCP Open
  Listen: CDPCP
  Open: IPCP
  Last input 00:00:01, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/10/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     20 packets input, 1605 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     4 input errors, 0 CRC, 4 frame, 0 overrun, 0 ignored, 0 abort
     23 packets output, 2403 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

Step 2 Confirm that the “LCP Open” line appears in the command output.

Step 3 To continue configuration, reenter global configuration mode.

Confirming the Asynchronous Line Configuration

Follow these steps to confirm the configuration of the asynchronous line:

Step 1 From the privileged EXEC mode, enter the **show line** command. You should see command output similar to the following:

```
Router# show line 1
Tty Typ     Tx/Rx     A Modem  Roty AccO AccI  Uses    Noise
Overruns
A  1 TTY  19200/19200  -    -      -    -    -     2        4
0/0

Line 1, Location: "", Type: ""
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 19200/19200, no parity, 1 stopbits, 8 databits
Status: Ready, Active, Async Interface Active, HW PPP Support Active
Capabilities: Line is permanent async interface
Modem state: Ready
Line is running PPP for address 192.168.39.40
0 output packets queued, 0 input packets.
 Async Escape map is 00000000000000000101000000000000
Modem hardware state: CTS DSR  DTR RTS
Special Chars: Escape  Hold  Stop  Start  Disconnect  Activation
               ^^x    none   -     -       none
```

Step 2 Confirm that the “Line 1” message appears in the command output.

The asynchronous line settings should be the same as those that you configured in the “Configuring the Asynchronous Interface” section on page 8-5.

The IP address in the “Line is running” message should be the IP address of the WAN interface of the central-site router.

Configuring When the Router Dials

Follow these steps to configure how and when the router dials the central-site router.

	Command	Task
Step 1	**interface Serial0**	Enter configuration mode for the serial interface.
Step 2	**dialer map snapshot** *1* **name** *HQ*	Define a dialer map for snapshot routing.
Step 3	**dialer map ip** *192.168.39.40* **name** *HQ* **modem-script dialout** *5552053*	Configure a dialer map to send IP data over the modem line to the central-site router.
Step 4	**dialer map ipx** *9876.0000.0c06.ecc6* **modem-script dialout** *5552053*	Configure a dialer map to send IPX data over the modem line to the central-site router.
Step 5	**ipx sap** *4 HQ* **server** *AA 1234.0000.0000.0001* **2**	Configure a route to IPX services, such as servers and printers, on the central-site network.
Step 6	**exit**	Exit configuration mode for this interface.

Configuring Command-Line Access to the Router

Follow these steps to configure parameters that control access to the router.

	Command	Task
Step 1	**line console** *0*	Specify the console terminal line.
Step 2	**exec-timeout** *5*	Set the interval (in minutes) that the EXEC command interpreter waits until user input is detected.
Step 3	**line vty** *0 4*	Specify a virtual terminal for remote console access.
Step 4	**password** *<lineaccess>*	Specify a password on the line.
Step 5	**login**	Enable password checking at terminal session login.
Step 6	**end**	Exit configuration mode.

Asynchronous Dial-In Pool

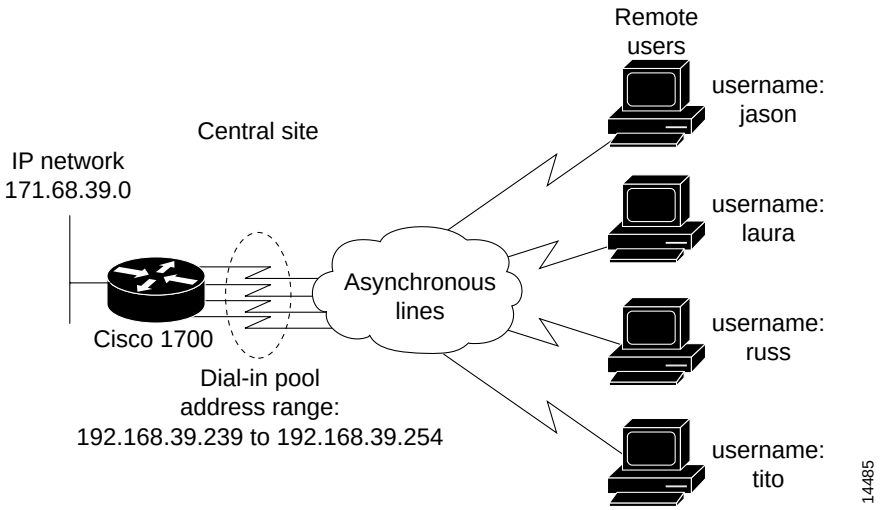
This section describes how to configure a Cisco router with multiple asynchronous interfaces for dial-in connections. In this example, the Cisco router functions as the central-site router that accepts connections from remote users.

These are the major task in configuring an asynchronous dial-in pool:

- Configuring Global Parameters
- Configuring Security
- Configuring the Fast Ethernet Interface
- Configuring the Asynchronous Interfaces
- Configuring Command-Line Access to the Router

Figure 8-2 shows the configuration example used in this section.

Figure 8-2 Configuration Example—Asynchronous Dial-In Pool



This configuration example includes multiple interfaces of the same type being configured with the same commands. When you enter commands for one of the multiple interfaces, you must enter interface configuration mode for the correct interface. Table 8-1 shows how the interfaces are numbered in this configuration example.

Table 8-1 Serial Interface Numbering

Line	Interface Name and Number
1	Serial0
2	Serial1
3	Serial2
4	Serial3
5 (AUX port)	Async5

Configuring Global Parameters

Follow these steps to configure global parameters.

	Command	Task
Step 1	**configure terminal**	Enter configuration mode.
Step 2	**service timestamps debug datetime msec**	Configure the router to show the date and time of all debug messages. This command is optional, but it is recommended if you use debug commands to troubleshoot your configuration.
Step 3	**service timestamps log datetime msec**	Configure the router to show the date and time of all log messages. This command is optional, but it is recommended if you use the verification steps described in this guide. This feature is enabled for all the command output examples shown in this guide.

Configuring Security

Follow these steps to configure the router with security measures.

	Command	Task
Step 1	**service password-encryption**	Configure the router to encrypt passwords.
Step 2	**enable password** <*user*>	Specify a password to prevent unauthorized access to the router.
Step 3	**hostname** *Router*	Configure the router with a host name, which is used in prompts and default configuration filenames. For PPP authentication, the host name entered with this command must match the username of the central-site router.
Step 4	**username** *jason* **password** <*foot*> **username** *laura* **password** <*letmein*> **username** *russ* **password** <*openup*> **username** *tito* **password** <*iamhere*>	Specify the password used during caller identification and CHAP and PAP authentication. For CHAP and PAP authentication, the host name of every remote router that dials into the router must be entered with this command, along with the password used to authenticate the router.

Configuring the Fast Ethernet Interface

Follow these steps to configure the Fast Ethernet interface, which connects the router to your local network.

	Command	Task
Step 1	**interface fastethernet0**	Enter configuration mode for the Fast Ethernet interface.
Step 2	**ip address** *192.168.39.1 255.255.255.0*	Configure this interface with an IP address and a subnet mask.

	Command	Task
Step 3	**no shutdown**	Enable the interface and the configuration changes that you have just made on the interface.
Step 4	**exit**	Exit configuration mode for the interface.

Configuring the Asynchronous Interfaces

Follow these steps to configure how the four asynchronous interfaces will receive calls from remote routers. The procedure below tells how to configure one interface (Serial0); however, you can use the same commands to configure any of the serial interfaces, as well as the AUX interface (Async5).

	Command	Task
Step 1	**interface serial0**	Enter configuration mode for the asynchronous serial interface.
Step 2	**ip unnumbered fastethernet0**	Configure the asynchronous interfaces to use the IP address of the FastEthernet interface.
Step 3	**encapsulation ppp**	Configure the asynchronous interfaces for PPP encapsulation.
Step 4	**async mode interactive**	Configure the asynchronous interfaces for interactive mode, which enables **slip** and **ppp** EXEC commands.
Step 5	**peer default ip address pool** *dialin*	Configure the remote routers to use the IP address configured with the **ip local pool** command.
Step 6	**no cdp enable**	Disable Cisco Discovery Protocol (CDP) on the asynchronous interfaces.
Step 7	ppp authentication chap	Configure the asynchronous interfaces to authenticate the remote routers with CHAP.
Step 8	**no shutdown**	Enable this interface and the configuration changes you have made.
Step 9	**exit**	Exit configuration mode for this interface.

	Command	Task
Step 10	**ip local pool** *dialin 192.168.39.239 192.168.39.254*	Configure a local pool of IP addressees that are used when a remote router connects to the one of the asynchronous interfaces. The command defines the range of IP address that can be used, with the lowest IP address followed by the highest IP address. If you do not include the highest IP address, the pool contains only the lowest IP address defined in the command.
Step 11	**line 1**	Enter configuration mode for the serial0 interface.
Step 12	**speed** *19200*	Configure the baud rate for the asynchronous line.
Step 13	**parity** *n*	Configure parity on the asynchronous line.
Step 14	**datab** *8*	Configure data bits on the asynchronous line.
Step 15	**stopb** *1*	Configure stop bits on the asynchronous line.
Step 16	**exit**	Exit line configuration mode.

Configuring Command-Line Access to the Router

Follow these steps to configure parameters that control access to the router.

	Command	Task
Step 1	**line console** *0*	Specify the console terminal line.
Step 2	**exec-timeout** *5*	Set the interval that the EXEC command interpreter waits until user input is detected.
Step 3	**line vty** *0 4*	Specify a virtual terminal for remote console access
Step 4	**password** <*lineaccess*>	Specify a password on the line.

	Command	Task
Step 5	**login**	Enable password checking at terminal session login.
Step 6	**end**	Exit configuration mode.

Troubleshooting Asynchronous Problems

If you are having problems or if the output that you received during the verification steps is very different from that shown in the command output examples, you can troubleshoot your router, using the Cisco IOS debug commands. The debug commands provide extensive command output that is not included in this document.

Caution If you are not familiar with Cisco IOS debug commands, you should read the "Using Debug Commands" section in the "Introduction to Router Configuration" chapter before attempting any debugging.

The following debug commands are helpful in troubleshooting asynchronous configurations. Follow these commands with the **ping** command to display debug output:

- **debug modem**
- **debug chat-script**
- **debug dialer**
- **debug ppp negotiation**

CHAPTER 9

Configuring X.25

This chapter describes how to configure the Cisco router to connect to a central-site router over an X.25 line or over an ISDN line and provides verification steps and troubleshooting tips.

This chapter contains the following sections:

- Before You Begin
- X.25
- X.25 over ISDN B Channel
- X.25 over ISDN D Channel
- Troubleshooting X.25 Problems

Before You Begin

The configurations in this chapter are based on the following assumptions:

- The router is connected a central-site router.
- You are routing IP and Internetwork Packet Exchange (IPX) network traffic.

Before you begin configuration, be aware of the following:

- You need to enter the commands in the order shown in the task tables.
- The values shown in italic are examples. You should substitute the values shown with values that are appropriate for your network.
- You should be familiar with Cisco IOS software and its conventions.

Note To use the verification steps described in this chapter, you must be familiar with Cisco IOS commands and command modes. When you use the verification steps, you need to change to different command modes. If you are not familiar with command modes, see the "Understanding Command Modes" section in the "Introduction to Router Configuration" chapter.

X.25

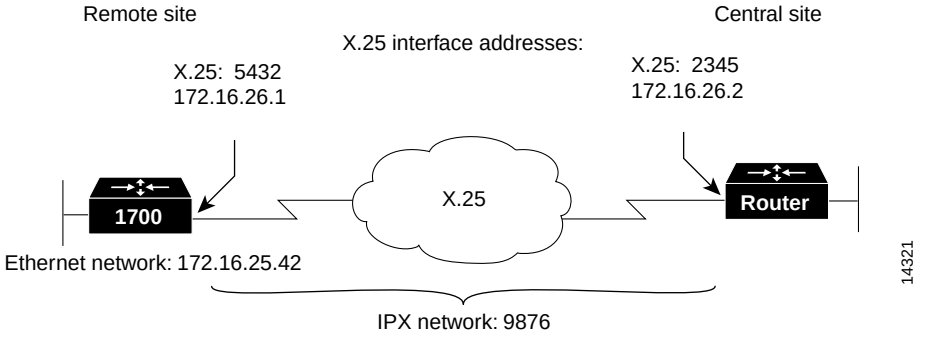
This section describes how to your router for a point-to-point X.25 WAN connection to the central-site router.

These are the major tasks in configuring your router:

- Configuring Global Parameters
- Configuring Security
- Configuring the Fast Ethernet Interface
- Configuring the X.25 Interface
- Configuring Command-Line Access to the Router

Figure 9-1 shows the configuration used in this example.

Figure 9-1 Configuration Example—X.25



Configuring Global Parameters

Follow these steps to configure the router for global parameters.

	Command	Task
Step 1	**configure terminal**	Enter configuration mode.
Step 2	**service timestamps debug datetime msec**	Configure the router to show the date and time of all debug messages. This command is optional, but it is recommended if you use debug commands to troubleshoot your configuration.
Step 3	**service timestamps log datetime msec**	Configure the router to show the date and time of all log messages. This command is optional, but it is recommended if you use the verification steps described in this guide. This feature is enabled for all the command output examples shown in this guide.
Step 4	**ipx routing** *0060.834f.66dd*	Enable IPX routing, and configure the router with an IPX address.

Configuring Security

Follow these steps to configure the router with security measures.

	Command	Task
Step 1	**hostname** *Router*	Configure the router with a host name, which is used in prompts and default configuration filenames. For Point-to-Point Protocol (PPP) authentication, the host name entered with this command must match the username of the central-site router.
Step 2	**enable password** <*user*>	Specify a password to prevent unauthorized access to the router.

Configuring the Fast Ethernet Interface

Follow these steps to configure the Fast Ethernet interface, which connects your router to the local network.

	Command	Task
Step 1	**interface fast ethernet0**	Enter configuration mode for the Ethernet interface.
Step 2	**ip address** *172.16.25.42 255.255.255.224*	Configure this interface with an IP address and a subnet mask.
Step 3	**ipx network** *ABC*	Configure this interface with an IPX network number.
Step 4	**no shutdown**	Enable the interface and the configuration changes that you have just made on the interface.
Step 5	**exit**	Exit configuration mode for this interface.

Configuring the X.25 Interface

Follow these steps to configure the X.25 interface, which connects your router to the central-site router over the wide-area network.

	Command	Task
Step 1	**interface Serial0**	Enter configuration mode for the serial interface.
Step 2	**ip address** *172.16.26.1 255.255.255.0*	Configure this interface with an IP address.
Step 3	**encapsulation x25**	Set the encapsulation type on this interface to X.25.
Step 4	**ipx network** *9876*	Enable IPX routing on this interface.
Step 5	**x25 address** *5432*	Set the X.121 address of this interface.
Step 6	**x25 map ip** *172.16.26.2 2345* **broadcast**	Set up the LAN protocols-to-remote-host mapping for IP and X.25.
Step 7	**x25 map ipx** *9876.0000.0c03.ecc6 2345* **broadcast**	Set up the LAN protocols-to-remote-host mapping for IPX and X.25.
Step 8	**no shutdown**	Enable the interface and the configuration changes that you have just made on the interface.
Step 9	**exit**	Exit configuration mode for this interface.

Verifying Your Configuration

You can verify your configuration to this point by

- Confirming Connectivity to the Central-Site Router over IP
- Confirming Connectivity to the Central-Site Router over IPX
- Confirming That the Serial Interface Is Functioning Correctly
- Confirming That the X.25 Map Is Configured Correctly
- Confirming Switched Virtual Circuit and Permanent Virtual Circuit Information

Confirming Connectivity to the Central-Site Router over IP

Follow these steps to confirm connectivity to the central-site router over IP:

Step 1 Confirm that the router is connected to the central-site router.

Step 2 From the privileged EXEC command mode, enter the **ping** command, followed by the IP address of the central-site router:

```
Router# ping 172.16.26.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echo to 192.168.39.41, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20
ms
```

Step 3 Confirm that the success rate shown in the output is 60 percent or greater. This means that your router is successfully transferring data to the central-site router.

Step 4 To continue configuration, reenter global configuration mode.

Confirming Connectivity to the Central-Site Router over IPX

Follow these steps to confirm connectivity to the central-site router over IPX:

Step 1 Confirm that the router is connected to the central-site router.

Step 2 From the privileged EXEC command mode, enter the **ping** command.

Step 3 Respond to the prompts shown in the following example, entering IPX as the protocol, and entering the target IPX address.

Note Substitute the IPX address of your central-site router for the IPX address shown in the example.

```
Router# ping
Protocol [ip]: ipx
Target IPX address: 9876.0000.0c03.ecc6
Repeat count [5]: <Return>
Datagram size [100]: <<Return>>
Timeout in seconds [2]: <<Return>>
Verbose [n]: <<Return>>
Novell Standard Echo [n]: <<Return>>
Type escape sequence to abort.
Sending 5, 100-byte IPX cisco Echoes to 9876.0000.0c03.ecc6, timeout
is 2 seconds: !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/21/24
ms
```

Step 4 Confirm that the success rate shown in the output is 60 percent or greater. This means that your router is successfully transferring data to the central-site router.

Step 5 To continue configuration, reenter global configuration mode.

Confirming That the Serial Interface Is Functioning Correctly

Follow these steps to confirm that the serial interface is functioning correctly:

Step 1 From the privileged EXEC command mode, enter the **show interface serial0** command. You should see command output similar to the following:

```
Router# show interface serial0

Serial0 is up, line protocol is up
Hardware is QUICC Serial
Internet address is 172.16.26.1/24
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation X25, loopback not set
x25 DTE, modulo 8, k 7, N1 12056, N2 20
T1 3000, interface outage (partial T3) 0, T4 0 State CONNECT, VS 6, VR
1, Remote VR 6, Retransmissions 0
Queues: U/S frames 0, I frames 0, unack. 0, reTx 0 IFRAMEs 22/25 RNRs
0/0 REJs 0/0 SABM/Es 0/1 FRMRs 0/0 DISCs 0/0 X25 DTE, address 5432,
state R1, modulo 8, timer 0
Defaults: cisco encapsulation, idle 0, nvc 1
input/output window sizes 2/2, packet sizes 128/128 Timers: T10 60,
T11 180, T12 60, T13 60, TH 0 Channels: Incoming-only none, Two-way
1-1024, Outgoing-only none RESTARTs 1/1 CALLs 1+0/2+2/0+0 DIAGs 0/0
Last input 00:00:32, output 00:00:32, output hang never Last clearing
of "show interface" counters never Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops 5 minute input
rate 0 bits/sec, 0 packets/sec 5 minute output rate 0 bits/sec, 0
packets/sec
40 packets input, 1903 bytes, 0 no buffer Received 0 broadcasts, 0
runts, 0 giants 2 input errors, 0 CRC, 2 frame, 0 overrun, 0 ignored,
0 abort 42 packets output, 2033 bytes, 0 underruns 0 output errors, 0
collisions, 11 interface resets 0 output buffer failures, 0 output
buffers swapped out 7 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
```

Step 2 Check that the "line protocol is up" and the "State CONNECT" messages appear in the command output. If you do not see these messages, see the "X.25 over ISDN B Channel" section on page 9-10 for suggestions.

Step 3 To continue configuration, reenter global configuration mode.

Confirming That the X.25 Map Is Configured Correctly

Follow these steps to confirm that the X.25 map is configured correctly:

Step 1 From the privileged EXEC command mode, enter the **show x25 map** command. You should see command output similar to the following:

```
Router# show x25 map

Serial0: X.121 2345 <--> ip 172.16.26.2,
ipx 9876.0000.0c03.ecc6
PERMANENT, BROADCAST, 1 VC: 1*
```

Step 2 Confirm that your IPX network number and the central-site router IP address and IPX address appear in the command output. The IP and IPX addresses shown in your output will be different from those shown in the example.

Confirming Switched Virtual Circuit and Permanent Virtual Circuit Information

Follow these steps to confirm the switched virtual circuit and permanent virtual circuit information:

Step 1 From the privileged EXEC command mode, enter the **show x25 vc** command, as follows. You should see command output similar to the following:

```
Router# show x25 vc
SVC 1, State: D1, Interface: Serial0
Started 00:04:10, last input 00:00:26, output 00:00:33 Connects 2345
<-->
ip 172.16.26.1
ipx 9876.0000.0c03.ecc6
multiprotocol cud pid, standard Tx data PID Window size input: 2,
output: 2
Packet size input: 128, output: 128
```

```
PS: 7 PR: 3 ACK: 3 Remote PR: 7 RCNT: 0 RNR: FALSE Retransmits: 0
Timer (secs): 0 Reassembly (bytes): 0 Held Fragments/Packets: 0/0
Bytes 1540/1724 Packets 15/19 Resets 0/0 RNRs 0/0 REJs 0/0 INTs 0/0
```

Step 2 Look for the following messages in the output:

- "SVC 1"—Means that the X.25 service is active for the X.25 interface.
- "State: D1"—Means that there is an active virtual circuit on the X. 25 interface.
- "Connects 2345 <-->"—Means that the X.25 address is correctly associated with the IP address and IPX address of the X.25 interface.
- "Packets 15/19"—Means that data is being transferred across the X.25 interface. The number shown in this message varies and shows the success rate of data that is being sent.

Step 3 To continue configuration, reenter global configuration mode.

Configuring Command-Line Access to the Router

Follow these steps to configure parameters that control access to the router.

	Command	Task
Step 1	**line console** *0*	Specify the console terminal line.
Step 2	**exec-timeout** *5*	Set the interval that the EXEC command interpreter waits until user input is detected.
Step 3	**line vty** *0 4*	Specify a virtual terminal for remote console access.
Step 4	**password** <*lineaccess*>	Specify a password on the line.
Step 5	**login**	Enable password checking at terminal session login.

X.25 over ISDN B Channel

This section describes how to configure the router to encapsulate IP and IPX packets as X.25 and how to route them over an ISDN B-channel connection.

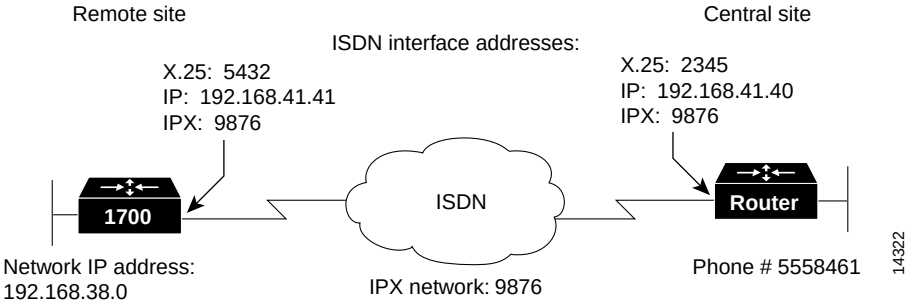
In addition to the assumptions described in the "Before You Begin" section in this chapter, this configuration is based on the assumption that you can only use one of the two ISDN B channels for this type of configuration.

These are the major tasks in configuring your router:

- Configuring Global Parameters
- Configuring Security
- Configuring the Fast Ethernet Interface
- Configuring the ISDN Interface for X.25
- Configuring Command-Line Access to the Router

Figure 9-2 shows the configuration used in this example.

Figure 9-2 Configuration Example—X.25 over ISDN B Channel



Configuring Global Parameters

Follow these steps to configure the router for global parameters.

	Commamd	Task
Step 1	**configure terminal**	Enter configuration mode.
Step 2	**service timestamps debug datetime msec**	Configure the router to show the date and time of all debug messages. This command is optional, but it is recommended if you use debug commands to troubleshoot your configuration.
Step 3	**service timestamps log datetime msec**	Configure the router to show the date and time of all log messages. This command is optional, but it is recommended if you use the verification steps described in this guide. This feature is enabled for all the command output examples shown in this guide.
Step 4	**ipx routing** *0060.834f.66dd*	Enable IPX routing, and configure the router with an IPX address.

	Commamd	Task
Step 5	**isdn switch-type** *basic-ni*	Configure the type of central office switch being used on the ISDN interface. Use the keyword that matches the ISDN switch type that you are using: • **basic-1tr6**—German 1TR6 ISDN switches • **basic-5ess**—Basic rate 5ESS switches • **basic-dms100**—NT DMS-100 basic rate switches • **basic-net3**—NET3 ISDN switches • **basic-ni**—National ISDN-1 switches • **basic-nwnet3**—Norway NET3 switches (phase 1) • **basic-nznet3**—New Zealand NET3 switches • **basic-ts013**—Australian TS013 switches • **ntt**—Japanese NTT ISDN switches • **vn2**—French VN2 ISDN switches • **vn3**—French VN3 ISDN switches
Step 6	**interface bri0**	Enter configuration mode for the ISDN interface.
Step 7	**no shutdown**	Enable the ISDN switch type configuration for the ISDN interface.
Step 8	**exit**	Exit configuration mode for the ISDN interface.

Verifying Your Configuration

You can verify your configuration to this point by confirming the ISDN line status as follows:

Step 1 From the privileged EXEC command mode, enter the **show isdn status** command. You should see command output similar to the following:

```
Router# show isdn status
The current ISDN Switchtype = basic-5ess
ISDN BRI0 interface
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 80, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        No Active Layer 3 Call(s)
    Activated dsl 0 CCBs = 0
    Total Allocated ISDN CCBs =
```

Step 2 Confirm that the "State = MULTIPLE_FRAME_ESTABLISHED" message appears in the command output, as shown in the example.

Note In some cases, you might see a "State = TEI_ASSIGNED" message instead of the "State = MULTIPLE_FRAME_ESTABLISHED" message. This message also means that the ISDN line is correctly configured.

Step 3 If you do not see the message, do the following:

a. Make sure that the router is correctly cabled.

b. Make sure that any external Network Termination 1 (NT1) equipment is functioning correctly. Refer to the documentation that came with the NT1.

c. Make sure that the ISDN line is correctly configured. Check with the ISDN service provider.

Step 4 To continue configuration, reenter global configuration mode.

Configuring Security

Follow these steps to configure the router with security measures.

	Command	Task
Step 1	**hostname** *Router*	Configure the router with a host name, which is used in prompts and default configuration filenames. For PPP authentication, the host name entered with this command must match the username of the central-site router.
Step 2	**enable password** <*user*>	Specify a password to prevent unauthorized access to the router.
Step 3	**username HQ password** <*guessme*>	Specify the password used during caller identification and Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) authentication. For CHAP and PAP authentication, the username entered with this command must match the host name of the central-site router.

Configuring the Fast Ethernet Interface

Follow these steps to configure the Fast Ethernet interface, which connects your router to the local network.

	Command	Task
Step 1	**interface fastethernet0**	Enter configuration mode for the Fast Ethernet interface.
Step 2	**ip address** *192.168.38.42 255.255.255.0*	Configure this interface with an IP address.

	Command	Task
Step 3	**no shutdown**	Enable the interface and the configuration changes that you have just made on the interface.
Step 4	**exit**	Exit configuration mode for this interface.

Configuring the ISDN Interface for X.25

Follow these steps to configure the ISDN interface, which connects your router to the central-site router over the wide-area network, for X.25 packet encapsulation.

	Command	Task
Step 1	**interface BRI0**	Enter configuration mode for the ISDN interface.
Step 2	**ip address** *192.168.41.41 255.255.255.0*	Configure this interface with an IP address.
Step 3	**encapsulation x25**	Set the encapsulation type on this interface to X.25.
Step 4	**snapshot client** *5 60*	Enable snapshot routing. Because your router is dialing into a central-site router, it is considered the client router. The first number is the amount of "active time" (in minutes) during which routing updates are exchanged between your router and the central-site router. The second number is the amount of "quiet time" (in minutes) during which routing entries are frozen and remain unchanged.
Step 5	**ipx network** *9876*	Enable IPX routing on this interface.
Step 6	**x25 address** *5432*	Set the X.25 address of this interface.
Step 7	**x25 map ip** *192.168.39.40 2345* **broadcast**	Set up the LAN protocols-to-remote-host mapping for X.25 to IP.
Step 8	**x25 map ipx** *9876.0000.0c03.ecc6 2345* **broadcast**	Set up the LAN protocols-to-remote-host mapping for IPX and X.25.

	Command	Task
Step 9	**dialer map ip** *192.168.39.40* **name** *HQ 5558461*	Configure this interface to place a call to multiple sites and to authenticate calls from multiple sites, based on IP address and dialer string. The name you enter after the **name** keyword in this command must match the name entered with the **username** command in the "Configuring Security" section on page 9-14.
Step 10	**dialer map ipx** *9876.0000.0c03.e336* **name** *HQ 5558461*	Configure this interface to place a call to multiple sites and to authenticate calls from multiple sites, based on IP address and dialer string. The name you enter after the **name** keyword in this command must match the name entered with the **username** command in the "Configuring Security" section on page 9-14.
Step 11	**dialer-group** *1*	Assign this interface to a dialer group.
Step 12	**dialer-list 1 protocol ip permit**	Define a dial-on-demand routing (DDR) dialer list to control dialing based on access lists and IP packets.
Step 13	**dialer-list 1 protocol ipx permit**	Define a DDR dialer list to control dialing based on access lists and IPX packets.

Verifying Your Configuration

You can verify your configuration to this point by

- Confirming Connectivity with the Central-Site Router over IP
- Confirming Connectivity to the Central-Site Router over IPX
- Confirming That the X.25 Map Is Configured Correctly
- Confirming Switched Virtual Circuit and Permanent Virtual Circuit Information

Confirming Connectivity with the Central-Site Router over IP

Follow these steps to confirm connectivity with the central-site router over IP:

Step 1 Confirm that your router X.25 connection is active.

Step 2 From the privileged EXEC command mode, enter the **ping** command, followed by the IP address of the central-site router. You should see command output similar to the following:

```
Router# ping 192.168.39.40

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echo to 192.168.39.40, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20
ms
```

Step 3 Confirm that the success rate shown in the output is 60 percent or greater. This means that your router is successfully transferring data to the central-site router.

Step 4 To continue configuration, reenter global configuration mode.

Confirming Connectivity to the Central-Site Router over IPX

Follow these steps to confirm connectivity with the central-site router over IPX:

Step 1 Confirm that your router X.25 connection is active.

Step 2 Enter the **ping** command, followed by the IPX address of the central-site router. You should see command output similar to the following:

```
Router# ping 9876.0000.0c03.ecc6
[ip]: ipx
IPX address: 105.0060.834f.667d
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Verbose [n]:
Type escape sequence to abort.5, 100-byte IPX cisco Echoes to
9876.0000.0c03.ecc6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Note Substitute the IPX address of your central-site router for the IPX address shown in the example.

Step 3 Confirm that the success rate shown in the output is 60 percent or greater. This means that your router is successfully transferring data to the central-site router.

Step 4 To continue configuration, reenter global configuration mode.

Confirming That the X.25 Map Is Configured Correctly

Follow these steps to confirm that the X.25 map is configured correctly:

Step 1 From the privileged EXEC command mode, enter the **show x25 map** command:

```
Router# show x25 map

Serial0: X.121 2345 <--> ip 192.168.39.40,
ipx 9876.0000.0c03.ecc6
PERMANENT, BROADCAST, 1 VC: 1*
```

Step 2 Confirm that the following appear in the command output:

- Your router IPX network number
- Central-site router IP address
- Central-site router IPX address

Note The IP and IPX addresses, and your router IPX network number shown in your output are different than those shown in the example.

Step 3 To continue configuration, reenter global configuration mode.

Confirming Switched Virtual Circuit and Permanent Virtual Circuit Information

Follow these steps to confirm switched virtual circuit and permanent virtual circuit information:

Step 1 From the privileged EXEC command mode, enter the **show x25 vc** command. You should see command output similar to the following:

```
Router# show x25 vc
SVC 1, State: D1, Interface: Serial0
Started 00:04:10, last input 00:00:26, output 00:00:33 Connects 2345
<-->
ip 192.168.39.40
ipx 9876.0000.0c03.ecc6
multiprotocol cud pid, standard Tx data PID Window size input: 2,
output: 2
Packet size input: 128, output: 128
PS: 7 PR: 3 ACK: 3 Remote PR: 7 RCNT: 0 RNR: FALSE Retransmits: 0
Timer (secs): 0 Reassembly (bytes): 0 Held Fragments/Packets: 0/0
Bytes 1540/1724 Packets 15/19 Resets 0/0 RNRs 0/0 REJs 0/0 INTs 0/0
```

Step 2 Confirm that the X.25 network number, shown in the "Connect" message, is associated with the correct IP and IPX addresses.

Step 3 To continue configuration, reenter global configuration mode.

Configuring Command-Line Access to the Router

Follow these steps to configure parameters that control access to the router.

	Command	Task
Step 1	**line console 0**	Specify the console terminal line.
Step 2	**exec-timeout** *5*	Set the interval that the EXEC command interpreter waits until user input is detected.
Step 3	**line vty** *0 4*	Specify a virtual terminal for remote console access.
Step 4	**password** <*lineaccess*>	Specify a password on the line.

	Command	Task
Step 5	**login**	Enable password checking at terminal session login.
Step 6	**end**	Exit configuration mode.

X.25 over ISDN D Channel

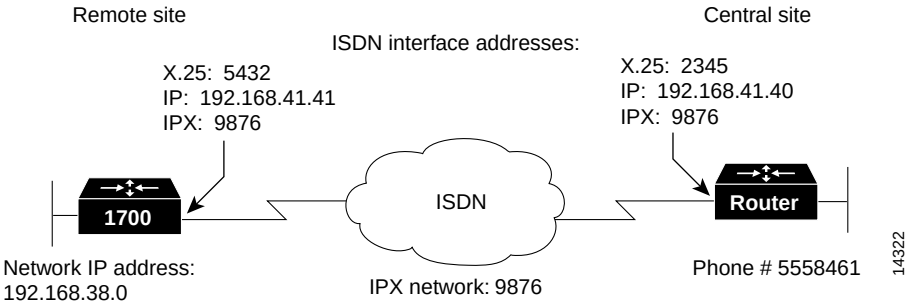
This section tells how to configure the router to send data as X.25 over an ISDN D-channel connection. This section also tells how to configure the router to encapsulate IP and IPX packets as X.25 and to then route them over an ISDN B-channel connection.

These are the major tasks in configuring your router:

- Configuring Global Parameters
- Configuring Security
- Configuring the Fast Ethernet Interface
- Configuring the ISDN Interface for X.25
- Configuring the ISDN Subinterface for X.25
- Configuring Command-Line Access to the Router

Figure 9-3 shows the configuration used in this example.

Figure 9-3 Configuration Example—X.25 over ISDN D Channel



Configuring Global Parameters

Follow these steps to configure global parameters.

	Command	Task
Step 1	**configure terminal**	Enter configuration mode.

	Command	Task
Step 2	**ipx routing** *0060.834f.66dd*	Enable IPX routing, and configure the router with an IPX address. If you do not know your router IPX address, you can enter this command without an address. The router then determines its own IPX address. You can then enter a **write terminal** command. The address will be displayed in the command output.
Step 3	**isdn switch-type** *basic-5ess*	Configure the type of central office switch being used on the ISDN interface. Use the keyword that matches the ISDN switch type that you are using: • **basic-1tr6**—German 1TR6 ISDN switches • **basic-5ess**—Basic rate 5ESS switches • **basic-dms100**—NT DMS-100 basic rate switches • **basic-net3**—NET3 ISDN switches • **basic-ni**—National ISDN-1 switches • **basic-nwnet3**—Norway NET3 switches (phase 1) • **basic-nznet3**—New Zealand NET3 switches • **basic-ts013**—Australian TS013 switches • **ntt**—Japanese NTT ISDN switches • **vn2**—French VN2 ISDN switches • **vn3**—French VN3 ISDN switches

Verifying Your Configuration

You can verify your configuration to this point by confirming the ISDN line status, as follows:

Step 1 Enter the **show isdn status** command. You should see command output similar to the following:

```
Router# show isdn status
The current ISDN Switchtype = basic-5ess
ISDN BRI0 interface
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 80, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        No Active Layer 3 Call(s)
    Activated dsl 0 CCBs = 0
    Total Allocated ISDN CCBs =
```

Step 2 Confirm that the "State = MULTIPLE_FRAME_ESTABLISHED" message appears in the command output.

Step 3 If you do not see the message, follow these steps:

a. Make sure that the router is correctly cabled.

b. Make sure that any external NT1 is functioning correctly. Refer to the documentation that came with the NT1.

c. Make sure the ISDN line is correctly configured by checking with the ISDN service provider.

d. See the "Troubleshooting X.25 Problems" section on page 9-29 for additional suggestions.

Configuring Security

Follow these steps to configure security measures.

	Command	Task
Step 1	**hostname** *Router*	Configure the router with a host name, which is used in prompts and default configuration filenames. For PPP authentication, the host name entered with this command must match the username of the remote device.
Step 2	**enable password** <*user*>	Specify a password to prevent unauthorized access to the router.

Configuring the Fast Ethernet Interface

Follow these steps to configure the Fast Ethernet interface, which connects your router to the local network.

	Command	Task
Step 1	**interface fastethernet0**	Enter configuration mode for the Fast Ethernet interface.
Step 2	**ip address** *192.168.38.42 255.255.255.0*	Configure this interface with an IP address.
Step 3	**no shutdown**	Enable the interface and the configuration changes that you have just made on the interface.
Step 4	**exit**	Exit configuration mode for this interface.

Configuring the ISDN Interface for X.25

Follow these steps to configure the ISDN, which connects your router to the central-site router over the wide-area network, for X.25 packet encapsulation.

	Command	Task
Step 1	**interface BRI0**	Enter configuration mode for the ISDN interface.
Step 2	**ip address** *192.168.40.41 255.255.255.0*	Configure this interface with an IP address.
Step 3	**encapsulation ppp**	Set the encapsulation method on this interface to PPP.
Step 4	**isdn x25 dchannel**	Create a configurable interface for X.25 traffic over the ISDN D channel.
Step 5	**isdn x25 static-tei** *1*	Configure a static ISDN Layer 2 terminal endpoint identifier (TEI) for X.25 over the ISDN D channel.
Step 6	**dialer map ip** *192.168.40.40* **name** *remote* **broadcast** *5558461* **dialer-group** *1*	Configure this interface to place a call to multiple sites and to authenticate calls from multiple sites, based on IP address and dialer string. The name you enter after the **name** keyword in this command must match the name entered with the **username** command in the "Configuring Security" section on page 9-22.
Step 7	**ppp authentication chap**	Enable CHAP or PAP authentication on this interface.
Step 8	**no shutdown**	Enable the interface and the configuration changes that you have just made on the interface.
Step 9	**exit**	Exit configuration mode for this interface.

Configuring the ISDN Subinterface for X.25

Follow these steps to configure an ISDN subinterface.

	Command	Task
Step 1	**interface BRI0:0**	Enter configuration mode for the ISDN subinterface.
Step 2	**ip address** *192.168.41.41 255.255.255.0*	Configure this interface with an IP address and a subnet mask.
Step 3	**encapsulation x25**	Set the encapsulation type on this interface to X.25.
Step 4	**ipx network** *9876*	Enable IPX routing on this interface.
Step 5	**x25 address** *5432*	Set the X.25 address of this interface.
Step 6	**dialer in-band**	Specify that DDR is supported on this interface.
Step 7	**x25 map ip** *192.168.41.40* **ipx** *9876.0000.0c03.ecc6 2345* **broadcast**	Set up the LAN protocols-to-remote-host mapping for IP and IPX.
Step 8	**dialer-list** *1* **protocol ip permit**	Define a DDR dialer list to control dialing based on access lists and IP packets.
Step 9	**no shutdown**	Enable the interface and the configuration changes that you have just made on the interface.
Step 10	**exit**	Exit configuration mode for this interface.

Verifying Your Configuration

You can verify your configuration to this point by

- Confirming Connectivity to the Remote Device over IP
- Confirming Connectivity to the Remote Device over IPX
- Confirming That the X.25 Map Is Configured Correctly
- Confirming Switched Virtual Circuit and Permanent Virtual Circuit Information

Confirming Connectivity to the Remote Device over IP

Follow these steps to confirm connectivity with the remote device over IP:

Step 1 Enter the **ping** command, followed by the IP address of the remote device. You should see command output similar to the following:

```
Router# ping 192.168.39.40

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 192.168.39.40, timeout is 2
seconds: !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20
ms
```

Step 2 Check the success rate in the command output. If the success rate is below 100 percent, see the "Troubleshooting X.25 Problems" section on page 9-29 for suggestions.

Confirming Connectivity to the Remote Device over IPX

Follow these steps to confirm connectivity with the remote device over IPX:

Step 1 Enter the **ping** command, and respond to the prompts shown in the following command output example:

```
Router# ping
Protocol [ip]: ipx
Target IPX address: 9876.0000.0c03.ecc6
Repeat count [5]: <Return>
Datagram size [100]: <<Return>>
Timeout in seconds [2]: <<Return>>
Verbose [n]: <<Return>>
Novell Standard Echo [n]: <<Return>>
Type escape sequence to abort.
Sending 5, 100-byte IPX cisco Echoes to 9876.0000.0c03.ecc6, timeout
is 2 seconds: !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/21/24
ms
```

Substitute the IPX address of your remote device for the IPX address shown in the example.

Step 2 Check the success rate in the command output. If the success rate is below 100 percent, refer to the following "Troubleshooting X.25 Problems" section for suggestions.

Note The modem might need time to synchronize with the central-site router. You might have to enter the **ping** command several times before you get a response.

Confirming That the X.25 Map Is Configured Correctly

Follow these steps to confirm that the X.25 map is configured correctly:

Step 1 Enter the **show x25 map** command. You should see command output similar to the following:

```
Router# show x25 map

Serial0: X.121 2345 <--> ip 192.168.39.40,
ipx 9876.0000.0c03.ecc6
PERMANENT, BROADCAST, 1 VC: 1*
```

Step 2 Confirm that your IPX network number and the remote device IP address and IPX address appear in the command output as shown in the example. The IP and IPX addresses shown in your output will be different from those shown in the example.

Confirming Switched Virtual Circuit and Permanent Virtual Circuit Information

Follow these steps to confirm the switched virtual circuit and permanent virtual circuit information:

Step 1 From the privileged EXEC command mode, enter the **show x25 vc** command. You should see command output similar to the following:

```
Router# show x25 vc
SVC 1, State: D1, Interface: Serial0
Started 00:04:10, last input 00:00:26, output 00:00:33 Connects 2345
<-->
```

```
ip 172.16.26.1
ipx 9876.0000.0c03.ecc6
multiprotocol cud pid, standard Tx data PID Window size input: 2,
output: 2
Packet size input: 128, output: 128
PS: 7 PR: 3 ACK: 3 Remote PR: 7 RCNT: 0 RNR: FALSE Retransmits: 0
Timer (secs): 0 Reassembly (bytes): 0 Held Fragments/Packets: 0/0
Bytes 1540/1724 Packets 15/19 Resets 0/0 RNRs 0/0 REJs 0/0 INTs 0/0
```

Step 2 Look for the following messages in the output:

- "SVC 1"—Means that the X.25 service is active for the X.25 interface.
- "State: D1"—Means that there is an active virtual circuit on the X. 25 interface.
- "Connects 2345 <-->"—Means that the X.25 address is correctly associated with the IP address and IPX address of the X.25 interface.
- "Packets 15/19"—Means that data is being transferred across the X.25 interface. The number shown in this message varies and indicates the success rate of data that is being transferred.

Configuring Command-Line Access to the Router

Follow these steps to configure parameters that control access to the router.

	Command	Task
Step 1	**line console** *0*	Specify the console terminal line.
Step 2	**exec-timeout** *5*	Set the interval (in minutes) that the EXEC command interpreter waits until user input is detected.
Step 3	**line vty** *0 4*	Specify a virtual terminal for remote console access.
Step 4	**password** *<lineaccess>*	Specify a password on the line.
Step 5	**login**	Enable password checking at terminal session login.
Step 6	**end**	Exit configuration mode.

Troubleshooting X.25 Problems

If you are having problems or if the output that you received during the verification steps is very different from that shown in the command output examples, you can troubleshoot your router by performing some or all of the following suggested actions.

Caution If you are not familiar with Cisco IOS debug commands, you should read the "Using Debug Commands" section in the "Introduction to Router Configuration" chapter before attempting any debugging.

- If the **ping** command is unsuccessful, use the **debug x25** command.
- If you cannot use the **ping** command to confirm connectivity to any device other than the central-site router, verify that your routing (static or dynamic) is correctly configured.
- If you do not see the "line protocol up" message in the **show interface** command output, use the **debug x25 event** command.
- If you do not see the "State CONNECT" message in the **show interface** command output, use the **debug lapb** command.
- For more detailed information than is contained in the **show isdn status** command output, use the **debug isdn q931** and **debug isdn q921** commands.

CHAPTER A

Networking Concepts

This appendix describes concepts that can help you in designing your network and in configuring your router in accordance with the examples in this guide.

This appendix contains the following sections:

- WAN Technologies
- CHAP and PAP Authentication
- Access Lists
- Dialer Interfaces and Dialer Profiles
- Network Address Translation
- Dynamic Host Configuration Protocol
- Virtual LANs

WAN Technologies

This section describes some of the WAN connection types that can be used with Cisco 1700 series routers, such as ISDN, Frame Relay, and X.25.

ISDN

ISDN is a set of digital services that is available through your local telephone company. ISDN digitizes information that is sent over the telephone network so that voice, data, text, graphics, music, video, and other material can be sent over existing telephone wire.

ISDN Components

ISDN components include terminals, terminal adapters (TAs), network termination devices, line-termination equipment, and exchange-termination equipment.

ISDN Terminals

There are two type of ISDN terminals:

- Terminal equipment type 1 (TE1) is designed specifically to work with ISDN. TE1s connect to the ISDN network with 4-wire, twisted-pair cable.
- Terminal equipment type 2 (TE2) is non-ISDN equipment (such as data terminal equipment [DTE]) that predates ISDN standards. TE2s connect to the ISDN network with a terminal adapter.

ISDN Network Termination Devices

Two types of ISDN terminal devices can connect your router to the telephone company's conventional 2-wire local loop:

- Network termination type 1 (NT1)—In North America, the NT1 is provided by the customer. In most other parts of the world, the NT1 is part of the network provided by the ISDN service provider. WAN interface cards that do not have an integrated NT1 must have an external NT1 in order to connect to ISDN services. The Cisco 1604 and ISDN BRI U WAN interface cards each have an integrated NT1.
- Network termination type 2 (NT2)—This more complicated device is usually found in digital private branch exchanges (PBXs).

There is also an NT1/2 device available that can perform the functions of both an NT1 and an NT2.

Services

There are two types of ISDN services:

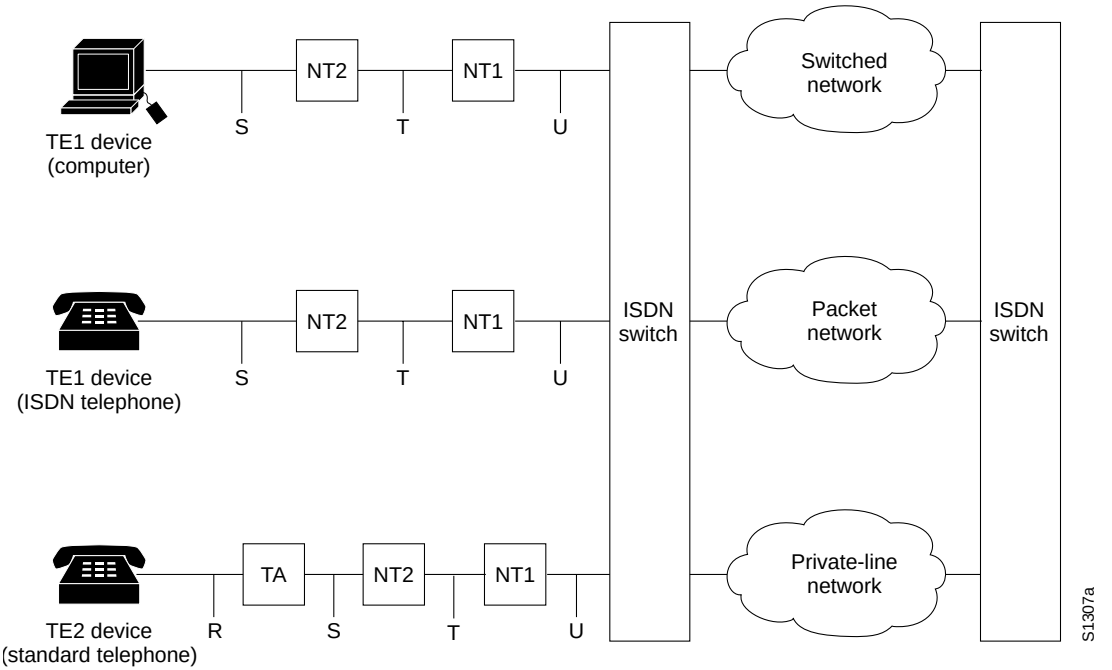
- Basic Rate Interface (BRI)—This service provides two B channels and one D channel. Each B channel operates at 64 kbps and carries user data. The D channel operates at 16 kbps and carries control and signaling information, although in certain circumstances it carries user data. BRI supports framing control and overhead, and the total bit rate is 192 kbps.
- Primary Rate Interface (PRI)—This service provides 23 B channels (which operate at 64 kbps) and 1 D channel (which operates at 64 kbps) in North America and Japan, resulting in a bit rate of 1.544 Mbps. In Europe, Australia, and other parts of the world, PRI provides 30 B channels, 1 D channel, and 1 maintenance/error channel. Each channel is 64 Kbps, for a total bit rate of 2.048 Mbps.

Sample Configuration

Figure 0-1 shows an example of ISDN configuration for various devices used to connect the user to the ISDN network.

Two of the devices shown, the computer and the ISDN telephone, are compatible with ISDN. The third device, the standard telephone, requires a TA to connect to the ISDN network through an NT1 or NT2 device.

Figure 0-1 Sample ISDN Network



Frame Relay

Frame Relay is a method of packet-switching that is used for communication between user devices (such as routers, bridges, and host machines) and network devices (such as switching nodes and modems). User devices are called *data terminal equipment* (DTE), and network devices are called *data circuit-terminating equipment* (DCE).

Frame Relay services can be provided by either a public network or a network of privately owned equipment serving a single enterprise.

Frame Relay is a streamlined, efficient, high-performance protocol. It is extremely fast because

- It multiplexes many logical data conversations (or virtual circuits) over one physical link. Multiplexing provides flexible and efficient use of bandwidth.

- It uses fiber media/digital transmission links. These types of physical connections have a high level of data integrity, so Frame Relay does not need to perform error checking. Error checking is time-consuming and can decrease WAN performance.
- It does not need to perform flow control procedures because these types of procedures are done by upper-layer protocols. Frame Relay uses a simple congestion notification mechanism to inform user devices when the network become congested. Congestion notification alerts the higher-layer protocols that flow control is needed.

Current Frame Relay standards support permanent virtual circuits (PVCs) that are configured and managed in a Frame Relay network. The Cisco 1700 router supports switched virtual circuits (SVCs) for DTE interfaces.

Frame Relay also has Local Management Interface (LMI) extensions for supporting large, complex internetworks. Any LMI extension known as *common* should be implemented in internetworks that support the LMI specification. Other LMI extensions are known as *optional*.

The LMI extensions are as follows:

- Virtual circuit status messages (common)—Provide communication and synchronization between the network and the user device, periodically report the addition of new PVCs and the deletion of existing PVCs, and provide information about PVC integrity.
- Multicasting (optional)—Allows a sender to transmit a single frame to multiple recipients, supporting the efficient routing of protocol messages and address resolution procedures that typically must be sent to many destinations simultaneously.
- Global addressing (optional)—Gives connection identifiers global rather than local significance, allowing them to be used to identify a specific interface to the Frame Relay network. Global addressing makes the Frame Relay network resemble a LAN, with respect to addressing.

X.25

X.25 is a method of packet switching that is used for communication between user devices (such as routers, bridges, and host machines) and network devices (such as switching nodes and modems). User devices are called *data terminal equipment* (DTE), and network devices are called *data circuit-terminating equipment* (DCE).

With X.25, one computer calls another to request a communication session. The called computer can accept or refuse the connection. If the call is accepted, the two computers begin full-duplex information transfer. Either computer can terminate the connection at any time.

User devices communicate with a bidirectional association called a *virtual circuit*. Devices on a network use virtual circuits to communicate through intermediate nodes without being directly, physically connected to each other. Virtual circuits are permanent or switched (temporary). PVCs are typically used for the most-often-used data transfers, and SVCs are used for sporadic data transfers.

BRI is an ISDN interface consisting of two B channels (B1 and B2) and one D channel. The B channels are used to transfer data, voice, and video. The D channel carries signal and call setup information. IPX, AppleTalk, transparent bridging, Xerox Network Systems (XNS), DECnet, and IP can all be encapsulated as X.25 over the ISDN B channels.

ISDN uses the D channel to carry signal information. ISDN can also use the D channel in a BRI to carry X.25 packets. The D channel has a capacity of 16 kbps; the X.25 over D channel can use up to 9.6 kbps.

You can set the parameters of the X.25-over-D-channel interface without disrupting the original ISDN interface configuration. In a normal ISDN BRI interface, the D and B channels are bundled together and represented as a single interface. The original BRI interface continues to represent the D, B1, and B2 channels.

Because some end-user equipment uses static terminal endpoint identifiers (TEIs) to access this feature, X.25 supports static TEIs. The dialer recognizes the X.25-over-D-channel calls and initiates them on a new interface.

X.25 traffic over the D channel can be used as a primary interface when low-volume, sporadic interactive traffic is the normal mode of operation. Supported traffic includes IP, IPX, AppleTalk, and transparent bridging.

CHAP and PAP Authentication

In configuring your router, you must select a method of authentication. Authentication is used for security and for identifying who is calling in so that the called router can correctly forward packets to the correct interface. This is generally required when dialer rotary groups are used and multiple sites are calling into a single router.

The configuration examples in this guide use Point-to-Point Protocol (PPP) with Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) for security and authentication. CHAP and PAP, when used with PPP encapsulation, allow routers to authenticate incoming calls.

CHAP Authentication

With CHAP, a remote device attempting to connect to the local router is requested, or challenged, to respond. When the local router receives the challenge response, it verifies the response by looking up the name of the remote device given in the response. The passwords must be identical on the remote device and the local router. The names and passwords are configured using the **username** command.

In the following example, Router Macbeth allows Router Macduff to call in using the password “bubble”:

```
hostname Macbeth
username Macduff password bubble
!
encapsulation ppp
ppp authentication chap
```

In the following example, Router Macduff allows Router Macbeth to call in using the password “bubble”:

```
hostname Macduff
username Macbeth password bubble
!
encapsulation ppp
ppp authentication chap
```

PAP Authentication

Like CHAP, PAP is an authentication protocol used with PPP. However, PAP is less secure. CHAP passes an encrypted version of the password on the physical link, but PAP passes the password and host name or username in clear text.

When interactive mode (rather than dedicated mode) is used on asynchronous lines, the **username** command allows a router to verify a username in an internal database before the user can call in to the router. In the following example, user Joe Smith is allowed to call in to the router if he uses the password "freedom":

```
username JoeSmith password freedom
line 1
login
```

Access Lists

Access lists control packet filtering on Cisco routers by limiting traffic and restricting network use by certain users or devices. Although there are several purposes for using access lists, the configuration examples in this guide use access lists to control the transmission of packets on a specific interface.

An access list is a sequential collection of "permit" and "deny" conditions that apply to network addresses. Packet addresses are compared to the conditions in all access lists configured in the router. The first match determines whether the packet is accepted or denied by the router. Because the router stops testing conditions after the first match, the order in which the conditions are defined in the access list is critical. If a packet does not match any conditions configured in an access list, the router rejects the packet.

For detailed information on how access lists work and how to configure them, refer to the "Configuring IP Services" chapter in the *Network Protocols Configuration Guide, Part 1*, publication, which is available on the Documentation CD-ROM that came with your router.

Dialer Interfaces and Dialer Profiles

A dialer interface is a WAN interface on the router that is not continuously connected to a remote device; it 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.

You can use dialer profiles to configure the router's physical interfaces 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 the same 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).
- An *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 Interfaces and Dialer Maps

A dialer interface configuration is a group of settings the routers 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 a 56-kbps ISDN speed, and the map class for a different destination might specify a 64-kbps ISDN speed.

Dialer Pools

Each dialer interface uses one group of physical interfaces, called a *dialer pool*. The physical interfaces in a dialer pool are ordered based on priority. One physical interface can belong to multiple dialer pools. ISDN BRI interfaces can set a limit

on the minimum and maximum number of B channels reserved by any dialer pool. A channel reserved by a dialer pool remains idle until traffic is directed to the pool.

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

Network Address Translation

Network Address Translation (NAT) provides a mechanism for a privately addressed network to access registered networks, such as the Internet, without requiring a registered subnet address. This mechanism eliminates the need for host renumbering and allows the same IP address range to be used in multiple intranets.

NAT is configured on the router at the border of an *inside network* (a network that uses nonregistered IP addresses) and an *outside network* (a network that uses a globally unique IP address; in this case, the Internet). NAT translates the inside local addresses (the nonregistered IP addresses assigned to hosts on the inside network) into globally unique IP addresses before sending packets to the outside network.

With NAT, the inside network continues to use its existing private or obsolete addresses. These addresses are converted into legal addresses before packets are forwarded onto the outside network. The translation function is compatible with standard routing; the feature is required only on the router connecting the inside network to the outside domain.

Translations can be static or dynamic. A static address translation establishes a one-to-one mapping between the inside network and the outside domain. Dynamic address translations are defined by describing the local addresses to be translated and the pool of addresses from which to allocate outside addresses. Allocation occurs in numerical order, and multiple pools of contiguous address blocks can be defined.

NAT eliminates the need to readdress all hosts that require external access, saving time and money. It also conserves addresses through application port-level multiplexing. With NAT, internal hosts can share a single registered IP address for

all external communications. In this type of configuration, relatively few external addresses are required to support many internal hosts, thus conserving IP addresses.

Because the addressing scheme on the inside network may conflict with registered addresses already assigned within the Internet, NAT can support a separate address pool for overlapping networks and translate the addresses as appropriate.

Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) is a client-server protocol that enables devices on an IP network (the DHCP clients) to request configuration information from a DHCP server. DHCP allocates network addresses from a central pool on an as-needed basis. DHCP is useful for assigning IP addresses to hosts connected to the network temporarily or for sharing a limited pool of IP addresses among a group of hosts that do not need permanent IP addresses.

DHCP frees you from having to manually assign an IP address to each client.

DHCP configures the router to forward User Datagram Protocol (UDP) broadcasts, including IP address requests, from DHCP clients. DHCP allows for increased automation and fewer network administration problems by

- Eliminating the need for the manual configuration of individual computers, printers, and shared file systems
- Preventing the simultaneous use of the same IP address by two clients
- Allowing configuration from a central site

Virtual LANs

A virtual LAN (VLAN) is a switched network that is logically segmented on an organizational basis, by functions, project teams, or applications, rather than on a physical or geographical basis. For example, all workstations and servers used by a particular workgroup team can be connected to the same VLAN, regardless of their physical connections to the network or the fact that they might be intermingled with other workgroup teams. Reconfiguration of the network can be done by means of software rather than by physically unplugging and moving devices or wires.

A VLAN can be thought of as a broadcast domain that exists within a defined set of switches. A VLAN consists of a number of end systems, either hosts or network equipment (such as bridges and routers), connected by a single bridging domain. The bridging domain is supported on various pieces of network equipment; for example, LAN switches that operate bridging protocols between them, with a separate bridge group for each VLAN.

VLAN Issues

VLANs are created to provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, address summarization, and traffic flow management. None of the switches within the defined group will bridge any frames, not even broadcast frames, between two VLANs. Several key issues need to be considered in designing and building switched LAN internetworks:

- LAN Segmentation
- Security
- Broadcast Control
- Performance
- Network Management

LAN Segmentation

VLANs allow logical network topologies to overlay the physical switched infrastructure in such a way that any arbitrary collection of LAN ports can be combined into an autonomous user group or community of interest. The technology logically segments the network into separate Layer 2 broadcast domains whereby packets are switched between ports designated to be within the same VLAN. By restricting traffic originating on a particular LAN only to other LANs in the same VLAN, switched virtual networks avoid wasting bandwidth, a drawback inherent to traditional bridged and switched networks in which packets are often forwarded to LANs with no need for them. Implementation of VLANs also improves scalability, particularly in LAN environments that support broadcast- or multicast-intensive protocols and applications that flood packets throughout the network.

Security

VLANs also improve security by isolating groups. High-security users can be grouped into a VLAN, possibly on the same physical segment, and no users outside that VLAN can communicate with them.

Broadcast Control

Just as switches isolate collision domains for attached hosts and forward only appropriate traffic out a particular port, VLANs provide complete isolation between VLANs. A VLAN is a bridging domain and all broadcast and multicast traffic is contained within it.

Performance

The logical grouping of users allows an accounting group to make intensive use of a networked accounting system assigned to a VLAN that contains just that accounting group and its servers. That group's work will not affect other users. The VLAN configuration improves general network performance by not slowing down other users sharing the network.

Network Management

The logical grouping of users allows easier network management. It is not necessary to pull cables to move a user from one network to another. Additions, moves, and changes are achieved by configuring a port into the appropriate VLAN.

Communicating Between VLANs

The Cisco 1700 series routers uses the IEEE 802.1Q protocol for routing between VLANs.

The IEEE 802.1Q protocol is used to interconnect multiple switches and routers and for defining VLAN topologies. IEEE 802.1Q support is currently available only for Fast Ethernet interfaces.

Procedures for configuring routing between VLANs with IEEE 802.1Q encapsulation are provided in Chapter 4, "Configuring Routing Among VLANs with IEEE 802.1Q Encapsulation."

VLAN Translation

VLAN translation refers to the ability of the Cisco IOS software to translate between different virtual LANs or between VLAN and non-VLAN encapsulating interfaces at Layer 2. Translation is typically used for selective inter-VLAN switching of non-routable protocols and for extending a single VLAN topology across hybrid switching environments. Translation also allows the bridging of VLANs on the main interface; the VLAN encapsulating header is preserved. Topology changes in one VLAN domain do not affect a different VLAN.

Designing Switched VLANs

By the time you are ready to configure routing between VLANs, you will already have defined them through the switches in your network. Issues related to network design and VLAN definition should be addressed during your network design. Refer to the *Cisco Internetworking Design Guide* and appropriate switch documentation for information on these topics:

- Sharing resources among VLANs
- Load balancing
- Redundant links
- Addressing
- Segmenting networks with VLANs

  Segmenting the network into broadcast groups improves network security. Use router access lists based on station addresses, application types, and protocol types.

- Routers and their role in switched networks

  In switched networks, routers perform broadcast management, route processing and distribution, and provide communications among VLANs. Routers provide VLAN access to shared resources and connection to other

parts of the network that are either logically segmented by means of the more traditional subnet approach or that require access to remote sites across wide-area links.

CHAPTER B

ROM Monitor

This appendix describes the Cisco router ROM monitor (also called the *bootstrap program*). The ROM monitor firmware runs when the router is powered up or reset. The firmware helps to initialize the processor hardware and boot the operating system software. You can perform certain configuration tasks, such as recovering a lost password or downloading software over the console port, by using the ROM monitor. If there is no Cisco IOS software image loaded on the router, the ROM monitor runs the router.

This appendix contains the following sections:

- Entering the ROM Monitor
- ROM Monitor Commands
- Command Descriptions
- Disaster Recovery with TFTP Download
- Configuration Register
- Console Download

Entering the ROM Monitor

To use the ROM monitor, you must be using a terminal or PC that is connected to the router by means of the console port. Refer to the installation chapter in the Hardware Installation Guide for your router, for information about connecting the router to a PC or terminal.

Follow these steps to configure the router to boot up in ROM monitor mode the next time it is rebooted.

	Command	Router Prompt	Task
Step 1	**enable**	`Router>`	If there is an enable password configured, enter the enable command and the enable password to enter privileged EXEC mode.
Step 2	**configure terminal**	`Router#`	Enter global configuration mode.
Step 3	**config-reg 0x0**	`Router(config)#`	Reset the configuration register.
Step 4	**exit**	`Router(config)#`	Exit global configuration mode.
Step 5	**reload**	`Router#`	Reboot the router with the new configuration register value. The router remains in ROM monitor and does not boot the Cisco IOS software. As long as the configuration value is 0x0, you must manually boot the operating system from the console. See the **boot** command in the "Command Descriptions" section on page B-4.
Step 6		`rommon 1>`	After the router reboots, it is in ROM monitor mode. The number in the prompt increments with each new line.

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

ROM Monitor Commands

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

```
rommon 1 > ?
alias               set and display aliases command
boot                boot up an external process
break               set/show/clear the breakpoint
confreg             configuration register utility
cont                continue executing a downloaded image
context             display the context of a loaded image
cookie              display contents of cookie PROM in hex
dev                 list the device table
dir                 list files in file system
dis                 display instruction stream
dnld                serial download a program module
frame               print out a selected stack frame
help                monitor builtin command help
history             monitor command history
meminfo             main memory information
repeat              repeat a monitor command
reset               system reset
set                 display the monitor variables
stack               produce a stack trace
sync                write monitor environment to NVRAM
sysret              print out info from last system return
tftpdnld            tftp image download
unalias             unset an alias
unset               unset a monitor variable
xmodem              x/ymodem image download
```

Commands are case sensitive. You can halt any command by pressing the Break key on a terminal. If you are using a PC, most terminal emulation programs halt a command when you press the Ctrl and the Break keys at the same time. If you are using another type of terminal emulator or terminal emulation software, refer to the documentation for that product for information on how to send a Break command.

Command Descriptions

Table B-1 describes commonly used ROM monitor commands.

Table 0-1 Common ROM Monitor Commands

Command	Description
help or **?**	Displays a summary of all available ROM monitor commands.

-?	Displays information about command syntax, for example:
	`rommon 16 > dis -?`
	`usage : dis [addr] [length]`
	
	The output for this command is slightly different for the **xmodem** download command:
	`rommon 11 > xmodem -?`
	`xmodem: illegal option -- ?`
	`usage: xmodem [-cyrx] destination filename`
	`-c  CRC-16`
	`-y  ymodem-batch protocol`
	`-r  copy image to dram for launch`
	`-x  do not launch on download completion`

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

dev	Lists boot device identifications on the router. For example:
	`rommon 2> dev`
	`Devices in device table:`
	`id  name`
	`flash: flash`
	`eprom:  eprom`

dir *device***:**	Lists the files on the named device (Flash, for example):
	`rommon 1> dir flash:`
	`File size  Checksum  File name`
	`7729736 bytes (0x75f248)  0xb86d`
	`c1700-bk9no3r2sy7-mz.0412`

Table B-2 describes the ROM monitor boot commands. For more information about the ROM monitor boot commands, refer to the *Cisco IOS Configuration Guide* and *Cisco IOS Command Reference* publications.

Table 0-2 Boot Commands

Command	Description
b	Boots the first image in Flash memory.
b flash: [*filename*]	Attempts to boot the image directly from the first partition of Flash memory. If you do not enter a filename, this command will boot the first image in Flash.
b flash:2: [*filename*]	Attempts to boot the image directly from the second partition of Flash memory. If you do not enter a filename, this command will boot the first image in the second partition of Flash memory.

Disaster Recovery with TFTP Download

The standard way to load new software on your router is using the **copy tftp flash** privileged EXEC command from the Cisco IOS software command-line interface (CLI). However, if the router is unable to boot the Cisco IOS software, you can load new software while in ROM monitor mode.

This section tells how, in ROM monitor mode, to download a Cisco IOS software image from a remote TFTP server to the router Flash memory. Use the **tftpdnld** command only for disaster recovery because it erases all existing data in Flash memory before downloading a new software image to the router.

Note A 10BASE-T Ethernet Port is not active in ROM monitor mode and, thus, cannot be used for TFTP download.

TFTP Download Command Variables

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

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

Required Variables

The following variables must be set with the commands shown before using the **tftpdnld** command:

Variable	Command
IP address of the router.	**IP_ADDRESS=** *ip_address*
Subnet mask of the router.	**IP_SUBNET_MASK=** *ip_address*
IP address of the default gateway of the router.	**DEFAULT_GATEWAY=** *ip_address*
IP address of the TFTP server from which the software will be downloaded.	**TFTP_SERVER=** *ip_address*
The name of the file that will be downloaded to the router.	**TFTP_FILE=** *filename*

Optional Variables

The following variables can be set with the commands shown before using the **tftpdnld** command:

Variable	Command
Whether or not the router performs a checksum test on the downloaded image: **1**—Checksum test is performed. **0**—No checksum test is performed.	**TFTP_CHECKSUM=***setting*

Variable	Command
Number of times the router attempts ARP and TFTP download. The default is 7.	**TFTP_RETRY_COUNT=** *retry_times*
Amount of time, in seconds, before the download process times out. The default is 2400 seconds (40 minutes).	**TFTP_TIMEOUT=** *time*
Configures how the router displays file download progress. **0**—No progress is displayed. **1**—Exclamation points (!!!) are displayed to indicate file download progress. This is the default setting. **2**—Detailed progress is displayed during the file download process. For example: Initializing interface. Interface link state up. ARPing for 1.4.0.1 ARP reply for 1.4.0.1 received. MAC address 00:00:0c:07:ac:01	**TFTP_VERBOSE=** *setting*

Using the TFTP Download Command

The steps described in this section should be performed while in ROM monitor mode.

Step 1 Use the appropriate commands to enter all the required variables and any optional variables.

Step 2 Enter the **tftpdnld** command as follows:

```
rommon 1 > tftpdnld [ -r ]
```

Note The **-r** variable is optional. Entering this variable downloads and boots the new software but does not save the software to Flash. You can then use the image that is in Flash the next time you enter the **reload** command in the Cisco IOS software CLI.

You will see output similar to the following:

```
IP_ADDRESS: 10.0.0.1
      IP_SUBNET_MASK: 255.255.0.0
     DEFAULT_GATEWAY: 1.3.0.1
         TFTP_SERVER: 223.255.254.254
           TFTP_FILE: c1700-bnr2sy-mz.070298
Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash will be lost!
Do you wish to continue? y/n:  [n]:
```

Step 3 If you are sure that you want to continue, enter **y** in response to the question in the output:

```
Do you wish to continue? y/n:  [n]:y
```

The router will begin to download the new file.

Pressing Ctrl-C or Break stops the transfer before the Flash memory is erased.

Configuration Register

The virtual configuration register is in NVRAM and has the same functionality as other Cisco routers. You can view or modify the virtual configuration register from either the ROM monitor or the operating system software.

To change the virtual configuration register from the ROM monitor, enter **confreg** by itself for menu mode, or enter the new value of the register in hexadecimal. For example:

confreg [*hexnum*]

This will change the virtual configuration register to the value specified. The value is always interpreted as hexadecimal. Entering **confreg** without an argument displays the contents of the virtual configuration register and a prompt to alter the contents by describing the meaning of each bit.

Whether or not an argument is provided, the new virtual configuration register value is written into NVRAM, but it does not take effect until you reset or power-cycle the router.

The following display shows an example of menu mode:

```
rommon 7> confreg

     Configuration Summary
enabled are:
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:  y
enable  "diagnostic mode"? y/n  [n]:  y
enable  "use net in IP bcast address"? y/n  [n]:
enable  "load rom after netboot fails"? y/n  [n]:
enable  "use all zero broadcast"? y/n  [n]:
enable  "break/abort has effect"? y/n  [n]:
enable  "ignore system config info"? y/n  [n]:
change console baud rate? y/n  [n]:  y
enter rate: 0 = 9600, 1 = 4800, 2 = 1200, 3 = 2400
 4 = 19200, 5 = 38400, 6 = 57600, 7 = 115200   [0]:  0
change the boot characteristics? y/n  [n]:  y
enter to boot:
 0 = ROM Monitor
 1 = the boot helper image
 2-15 = boot system
    [0]:  0

Configuration Summary
enabled are:
diagnostic mode
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:


You must reset or power cycle for new config to take effect
```

Console Download

You can use console download, a ROM monitor function, to download over the router console port either a software image or a configuration file. After downloading, the file is saved either to Flash memory or to main memory for execution (image files only).

Use console download when you do not have access to a TFTP server.

Note If you want to download a software image or a configuration file to the router over the console port, you must use the ROM monitor command.

Note If you are using a PC to download a Cisco IOS image over the router console port at 115,200 bps, ensure that the PC serial port is using a 16550 universal asynchronous receiver/transmitter (UART). If the PC serial port is not using a 16550 UART, we recommend using a speed of 38,400 or lower when downloading a Cisco IOS image over the console port.

Command Description

The following are the syntax and argument descriptions for the **xmodem** console download command.

The syntax is as follows:

xmodem [**-cyrx**] *destination_file_name*

The argument descriptions are as follows:

Argument	Description
c	Optional. Performs the download using 16-bit cyclic redundancy check (CRC) error checking to validate packets. Default is 8-bit CRC.

Argument	Description
y	Optional. Sets the router to perform the download using ymodem protocol. Default is xmodem protocol. The protocols differ as follows: • The xmodem protocol supports a 128-block transfer size, whereas the ymodem protocol supports a 1024-block transfer size. • The ymodem protocol uses 16-bit CRC error checking to validate each packet. Depending on the device that the software is being downloaded from, this function might not be supported by the xmodem protocol.
r	Optional. Image is loaded into DRAM for execution. Default is to load the image into Flash memory.
x	Optional. Image is loaded into DRAM without being executed.
destination_file_name	The name of the system image file or the system configuration file. In order for the router to recognize it, the name of the configuration file must be *router_confg*.

Error Reporting

Because the ROM monitor console download uses the console to perform the data transfer, error messages are displayed on the console only when the data transfer is terminated.

If an error does occur during a data transfer, the transfer is terminated, and an error message is displayed. If you have changed the baud rate from the default rate, the error message is followed by a message telling you to restore the terminal to the baud rate specified in the configuration register.

Debug Commands

Most ROM monitor debugging commands are functional only when Cisco IOS software has crashed or stopped. If you enter a debugging command and Cisco IOS crash information is not available, you see the following error message:

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

The following are ROM monitor debugging commands:

- **stack** or **k**—Produce a stack trace. For example:

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

- **context**—Display processor context. For example:

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

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

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

- **meminfo**—Display size in bytes, starting address, available range of main memory, the starting point and size of packet memory, and size of nonvolatile random-access memory (NVRAM). For example:

```
rommon 3> meminfo

Main memory size: 64 MB.
Available main memory starts at 0x10000, size 65472KB
IO (packet) memory size: 25 percent of main memory.
NVRAM size: 32KB
```

A

B

C

D

E

F

H

I

L

M

N

P

R

S

T

U

V

W

X