Cisco 806 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-7810437=
Text Part Number: 78-10437-01

Cisco 806 Router Software Configuration Guide

CHAPTER 3

APPENDIX B

APPENDIX C

Preface

This preface discusses the audience, organization, and conventions used in this guide. It also provides information on how to access other Cisco documentation that is available on the Cisco website, and how to order the Cisco Documentation CD-ROM.

Audience

This guide is intended for network administrators whose backgrounds vary from having no or little experience configuring routers to having a high level of experience. This guide is useful for both the following situations:

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

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

See the "Organization" section on page xii to find out which chapter contains the information you need to configure your software.

Organization

This guide is organized as follows:

- Chapter 1, “Concepts”—Provides general concept explanations of the features in the Cisco 806 router.
- Chapter 2, “Network Scenarios”—Describes a number of Internet access scenarios, with their specific network topologies and configurations.
- Chapter 3, “Feature-by-Feature Router Configuration”—Explains the Cisco 806 router configuration, feature by feature.
- Chapter 4, “Troubleshooting”—Provides information on identifying and solving problems with the Ethernet interfaces. Also explains how to recover a lost software password.
- Appendix A, “Cisco IOS Basic Skills”—Explains what you need to know about the Cisco IOS software before you begin to configure it.
- Appendix B, “ROM Monitor”—Explains how to use the ROM Monitor bootstrap program to reinitialize the Cisco 806 hardware and perform configuration tasks.
- Appendix C, “Common Port Assignments”—Describes the currently assigned Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) port numbers.

Conventions

This section describes the conventions used in this guide.

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

  For example, the key combinations ^D and Ctrl-D are equivalent. Both mean to hold down the Control key while pressing the D key. Keys are indicated in capitals, but are not case sensitive.

Command descriptions use these conventions:

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

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

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

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

Related Documents

The following publications provide related information on this product:

- *Cisco 806 Router Cabling and Setup Quick Start Guide* is a guide to quickly cabling and setting up the Cisco 806 router.
- *Cisco 806 Router Hardware Installation Guide* is the detailed guide for installing the Cisco 806 router.
- *Cisco Router Web Setup User Guide* explains how to use the Cisco Router Web Setup application.
- *Release Notes for the Cisco 806 Router* contains the latest information about the Cisco 806 router.
- The latest version of the *Cisco IOS Release Notes* contains information about the Cisco IOS images available for the Cisco 806 router.
- *Regulatory Compliance and Safety Information for the Cisco 806 Router* provides regulatory compliance and safety information for the Cisco 806 router.

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

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

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package. 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 as 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, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

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

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:

Attn Document Resource Connection
Cisco Systems, Inc.
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. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

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

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

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

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

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

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

Concepts

This chapter contains conceptual information that may be useful to Internet service providers and network administrators when configuring the Cisco 806 router. To review some typical network scenarios, read Chapter 2, “Network Scenarios.” For information on specific configurations, read Chapter 3, “Feature-by-Feature Router Configurations.”

The following topics are included in this chapter:

- Cisco 806 Router Overview
- Network Protocols
- Routing Protocol Options
- Policy-Based Routing
- IP Multicasting
- Point-to-Point Protocol over Ethernet
- Security Features
- Ethernet
- Network Address Translation
- Internet Protocol Control Protocol
- Dynamic Host Configuration Protocol Client and Server
- NetMeeting
- Network Time Protocol Server
- Service Assurance Agent

Cisco 806 Router Overview

The Cisco 806 router is a Cisco IOS-based member of the Cisco 800 router family. The router is a fixed-configuration IP router with security features to provide a secure Ethernet gateway for users in small offices, branch offices and home offices using broadband access to the Internet. It is designed to work with digital subscriber line (DSL), cable, or long-reach Ethernet (LRE) modems, or with an Ethernet switch serving a multitenant unit.

Among the features that the Cisco 806 router supports are IP Security (IPSec), NetMeeting, and IP multicasting. Users in remote locations using a public network can exchange data, access corporate intranets, participate in video conferences using their web browsers, and access corporate multicast material such as distance learning courses and videotaped presentations.

The Cisco 806 router has four 10BaseT Ethernet ports that function as a hub; this router also has one 10BaseT Ethernet wide area network (WAN) port.

Cisco 806 router Flash memory includes Webflash, which is a 2-Megabyte partition separate from system Flash. Webflash is only used by the Cisco Router Web Setup software.

Network Protocols

Network protocols enable the network to pass data from its source to a specific destination over LAN or WAN links. The Cisco 806 router supports the Internet Protocol (IP). To enable the transport of other protocols over IP, the Cisco 806 router supports Generic routing encapsulation (GRE) tunneling protocol.

IP

The best known Transmission Control Protocol/Internet Protocol (TCP/IP) at the internetwork layer is IP, which provides the basic packet delivery service for all TCP/IP networks. In addition to the physical node addresses, the IP implements a system of logical host addresses called *IP addresses*. The IP addresses are used by the internetwork and higher layers to identify devices and to perform internetwork routing. The Address Resolution Protocol (ARP) enables IP to identify the physical address that matches a given IP address.

IP is used by all protocols in the layers above and below it to deliver data, which means that all TCP/IP data flows through IP when it is sent and received, regardless of its final destination.

IP is a connectionless protocol, which means that IP does not exchange control information (called a *handshake*) to establish an end-to-end connection before transmitting data. In contrast, before sending data, a connection-oriented protocol first exchanges control information with the remote computer to verify that it is ready to receive data. When the handshaking is successful, the computers have established a connection. IP relies on the upper layer protocol TCP to establish the connection if connection-oriented services are required.

GRE Tunneling Protocol

GRE is a tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP network. By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling using GRE allows network expansion across a single-protocol backbone environment. GRE tunneling is commonly used in conjunction with IPSec.

Layer 2 Tunneling Protocol

Layer 2 Tunnel Protocol (L2TP) is an Internet Engineering Task Force (IETF) protocol that provides tunneling of Point-to-Point Protocol.

Routing Protocol Options

Supported routing protocols include the following:

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

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

Table 1-1 RIP and Enhanced IGRP Comparison

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

RIP

RIP is an associated protocol for IP, and is widely used for routing Internet protocol traffic. RIP is a distance-vector routing protocol, which means that it uses distance (hop count) as its metric for route selection. *Hop count* is the number of routers that a packet must traverse to reach its destination. For example, if a particular route has a hop count of 2, then a packet must traverse two routers to reach its destination.

By default, RIP routing updates are broadcast every 30 seconds. You can reconfigure the interval at which the routing updates are broadcast. You can also configure triggered extensions to RIP so that routing updates are sent only when the routing database is updated. For more information on triggered extensions to RIP, refer to the Cisco IOS Release 12.0(1)T documentation set.

Enhanced IGRP

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

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

Because Enhanced IGRP supports IP, you can use one routing protocol for multiprotocol network environments, thus minimizing the size of the routing tables and the amount of routing information.

Policy-Based Routing

Policy-based routing (PBR) can be used when administrative issues dictate that traffic be routed through specific paths. By using policy-based routing, customers can implement policies that selectively cause packets to take different paths.

PBR also provides a mechanism for marking packets so that certain kinds of traffic receive differentiated, preferential service when used in combination with queuing techniques enabled through the Cisco IOS software. These queuing techniques are extremely powerful, simple, and flexible tools for network managers who implement routing policies in their networks.

PBR provides a mechanism for expressing and implementing forwarding/routing of data packets, based on the policies defined by the network administrators. It provides a more flexible mechanism for routing packets than the existing mechanism provided by routing protocols that use the destination of the packet to route it.

Routers forward packets to the destination addresses, based on information from static routes or dynamic routing protocols such as RIP, Open Shortest Path First (OSPF), or Enhanced IGRP. Instead of routing by the destination address, policy-based routing allows network administrators to determine and implement routing policies to allow or deny paths based on the following:

- Identity of a particular end system
- Application

- Protocol
- Size of packets

IP Multicasting

IP multicasting is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to thousands of corporate recipients and homes. Applications that take advantage of multicasting include video conferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news.

Without multicasting, these applications must be run by two inefficient schemes—unicasting and broadcasting. In unicasting, one copy of data is sent to each receiver. Although unicasting is a simple mechanism for one-to-one communication, it demands too much bandwidth from the network for one-to-many communication. In broadcasting, a single copy of data is sent to every user in the network, circumventing the bandwidth problem. However, it is not suitable if only few receivers requested the data.

IP multicasting solves the inherent bottlenecks created when you need information transferred from a single sender to multiple recipients. By sending only one copy of the information to the network and letting the network intelligently replicate the packet only where it was requested, you conserve bandwidth and network resources on both the sending end and the receiving end of a transmission.

Point-to-Point Protocol over Ethernet

The Point-to-Point Protocol (PPP) encapsulates network layer protocol information over point-to-point links. Point-to-Point Protocol over Ethernet (PPPoE) allows a PPP session to be initiated on a simple bridging Ethernet-connected client.

PPP originally emerged as an encapsulation protocol for transporting IP traffic over point-to-point links. PPP also established a standard for the assignment and management of IP addresses, asynchronous (start/stop) and bit-oriented synchronous encapsulation, network protocol multiplexing, link configuration, link quality testing, error detection, and option negotiation for such capabilities as network-layer address negotiation and data-compression negotiation. PPP supports these functions by providing an extensible link control protocol (LCP) and a family of Network Control Protocols (NCPs) to negotiate optional configuration parameters and facilities.

The current implementation of PPP supports two security authentication protocols to authenticate a PPP session:

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

PPPoE with PAP or CHAP authentication is often used to inform the central site which remote routers are connected to it.

PAP

PAP uses a two-way handshake to verify the passwords between routers. To illustrate how PAP works, imagine a network topology in which a remote office Cisco 806 router is connected to a corporate office Cisco 3600 router. After the PPP link is established, the remote office router repeatedly sends a configured username and password until the corporate office router accepts the authentication.

PAP has the following characteristics:

- The password portion of the authentication is sent across the link in clear text (not scrambled or encrypted).
- PAP provides no protection from playback or repeated trial-and-error attacks.
- The remote office router controls the frequency and timing of the authentication attempts.

CHAP

CHAP uses a three-way handshake to verify passwords. To illustrate how CHAP works, imagine a network topology in which a remote office Cisco 806 router is connected to a corporate office Cisco 3600 router.

After the PPP link is established, the corporate office router sends a challenge message to the remote office router. The remote office router responds with a variable value. The corporate office router checks the response against its own calculation of the value. If the values match, the corporate office router accepts the authentication. The authentication process can be repeated anytime after the link is established.

CHAP has the following characteristics:

- The authentication process uses a variable challenge value rather than a password.
- CHAP protects against playback attack through the use of the variable challenge value, which is unique and unpredictable. Repeated challenges limit the time of exposure to any single attack.
- The corporate office router controls the frequency and timing of the authentication attempts.

Note Cisco recommends using CHAP because it is more secure than PAP.

Security Features

This section discusses the security features available on the Cisco 806 router. It discusses the following features:

- IPSec
- Access Lists
- Remote Authentication Dial-In User Service
- Terminal Access Controller Access Control System Plus

IPSec

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. IPSec provides a necessary component of a standards-based, flexible solution for deploying a network-wide security policy.

Cisco’s implementation of IPSec uses the Data Encryption Standard (DES) and triple DES.

Access Lists

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

Remote Authentication Dial-In User Service

Remote Authentication Dial-In User Service (RADIUS) is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

RADIUS is a fully open protocol, distributed in source code format, that can be modified to work with any security system available on the market.

Cisco supports RADIUS under its AAA security paradigm. RADIUS can be used with other AAA security protocols, such as Terminal Access Controller Access Control System Plus (TACACS+), Kerberos, or local username lookup.

Use RADIUS in the following network environments that require access security:

- Networks with multiple-vendor access servers, each supporting RADIUS—For example, access servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendors’ access servers, dial-in users are authenticated through a RADIUS server that has been customized to work with the Kerberos security system.
- Networks already using RADIUS—You can add a Cisco router with RADIUS to the network. This might be the first step when you make a transition to a TACACS+ server.

- Networks in which a user must access only a single service—Using RADIUS, you can control user access to a single host, to a single utility such as Telnet, or to a single protocol such as PPP. For example, when a user logs in, RADIUS indentifies this user as having authorization to run PPP using IP address 10.2.3.4, and the defined access list is then started.
- Networks that require resource accounting—You can use RADIUS accounting independent of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session. An Internet service provider (ISP) might use a freeware-based version of RADIUS access control and accounting software to meet special security and billing needs.

RADIUS is not suitable in the following network security situations:

- Multiprotocol access environments—RADIUS does not support the following protocols:
  - AppleTalk Remote Access Protocol (ARAP)
  - NetBIOS Frame Protocol Control Protocol (NBFCP)
  - NetWare Asynchronous Services Interface (NASI)
  - X.25 packet assembler/disassembler (PAD) connections.
- Router-to-router situations—RADIUS does not provide two-way authentication. RADIUS can be used to authenticate from one router to a non-Cisco router if the non-Cisco router requires RADIUS authentication.
- Networks using a variety of services—RADIUS generally binds a user to one service model.

Terminal Access Controller Access Control System Plus

Cisco 806 routers support the Terminal Access Controller Access Control System Plus (TACACS+) protocol through Telnet. TACACS+ is a Cisco proprietary authentication protocol that provides remote access authentication and related network security services, such as event logging. User passwords are administered in a central database rather than in individual routers. TACACS+ also provides support for separate modular authentication, authorization, and accounting (AAA) facilities that are configured at individual routers.

Ethernet

The Cisco 806 router supports two Ethernet network interfaces. Ethernet is a baseband LAN protocol that transports data and voice packets to the WAN interface using carrier sense multiple access collision detect (CSMA/CD). The term is now often used to refer to all CSMA/CD LANs. Ethernet was designed to serve in networks with sporadic, occasionally heavy traffic requirements, and the IEEE 802.3 specification was developed in 1980, based on the original Ethernet technology.

Under the Ethernet CSMA/CD media-access process, any host on a CSMA/CD LAN can access the network at any time. Before sending data, CSMA/CD hosts listen for traffic on the network. A host wanting to send data waits until it detects no traffic before it transmits. Ethernet allows any host on the network to transmit whenever the network is quiet. A collision occurs when two hosts listen for traffic, hear none, and then transmit simultaneously. In this situation, both transmissions are damaged, and the hosts must retransmit at some later time. Algorithms determine when the colliding hosts should retransmit.

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 as appropriate.

NAT supports H.323 signaling for the Netmeeting application.

Internet Protocol Control Protocol

NAT and PPP/Internet Protocol Control Protocol (IPCP) enable a Cisco router to automatically negotiate its own registered WAN interface IP address from a central server and make it possible for all remote hosts to access the Internet using this single registered IP address. Because existing port-level multiplexed NAT functionality within the Cisco IOS software is used, IP addresses on the remote LAN are invisible to the Internet.

With PPP/IPCP, the Cisco 806 router automatically negotiates a globally unique (registered) IP address for the dialer interface from the ISP router.

Dynamic Host Configuration Protocol Client and Server

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

Note When NAT is used, DHCP relay cannot be used on the Cisco 806 router. The built-in DHCP server should be used instead.

NetMeeting

Microsoft NetMeeting is a conferencing tool that enables individuals to hold meetings with each other from their computers. Individuals using computers with the NetMeeting software and an Internet or LAN connection can hold meetings remotely, using such tools as a shared whiteboard, application and document sharing, file transfers, and (with the necessary hardware) audio and video conferencing.

The Cisco 806 router supports H.323 signaling for NetMeeting. Refer to the Cisco IOS documentation set for specific NetMeeting support information.

Network Time Protocol Server

The Network Time Protocol (NTP) provides a synchronized time base for networked routers, servers, and other devices. It also coordinates the time of network events, which aids in understanding and troubleshooting the time sequence of network events. For example, call records for specific users can be correlated within one millisecond. Using information from an NTP server, you can compare time logs from different networks, which is essential for tracking security incidents, analyzing faults, and troubleshooting.

Service Assurance Agent

The Service Assurance Agent (SA Agent) is both an enhancement to and a new name for the Response Time Reporter (RTR) feature that was introduced in Cisco IOS Release 11.2. The feature allows you to monitor network performance by measuring key Service Level Agreement (SLA) metrics such as response time, network resources, availability, jitter, connect time, packet loss and application performance. With Cisco IOS Release 12.0(5)T, the SA Agent provides new capabilities that enable you to

- Monitor the Domain Name Server, DHCP Server, and data-link switching (DLSw) peer stack and tunnel performance. Thresholds can be used to trigger additional collection of time delay statistics.
- Monitor network one-way delay variance (jitter) and packet loss.
- Monitor web server response time.

Network Scenarios

This chapter includes several network scenarios and their configurations for the Cisco 806 router. This chapter is useful if you are building a new network and want some guidance. If you already have a network set up and you want to add specific features, see Chapter 3, “Feature-by-Feature Router Configurations.”

The following scenarios are included:

- Virtual Private Network
- Small Office/Telecommuter with Basic Security
- Small Office/Telecommuter with Business-Class Security
- Small Office/Telecommuter with Business-Class Security and Enterprise Applications
- Ethernet Gateway

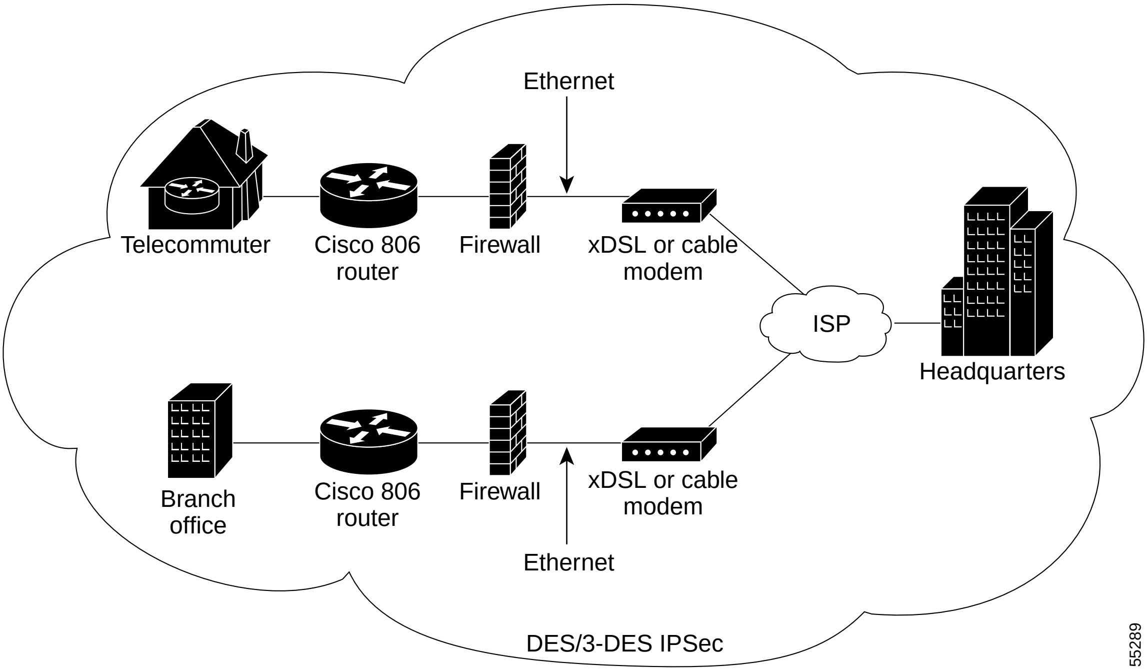
Each scenario is described in this chapter; a network diagram and configuration network examples are provided as models on which you can pattern your network. They cannot, however, anticipate all of your network needs. You can choose not to use features presented in the examples, or you can choose to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

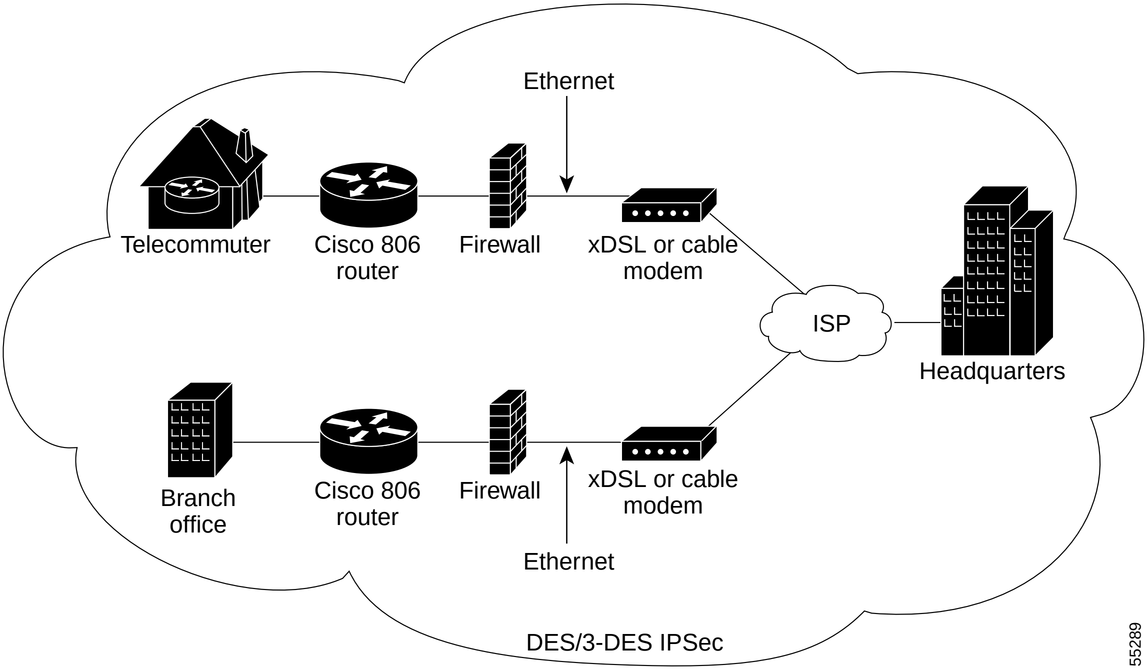
Note When you configure Ethernet interfaces, be aware that Ethernet 0 is the interface for hubbed ETHERNET ports 1 through 4, which support the local area network (LAN) on the premises, and Ethernet 1 is the interface for the INTERNET ETHERNET port.

Virtual Private Network

Figure 2-1 shows how the Cisco 806 router can be used in a virtual private network (VPN). The Cisco 806 router is linked to the Internet service provider (ISP) via a digital subscriber line (DSL) or a cable modem. Security is provided via IP security (IPSec) configuration.

Figure 2-1 Virtual Private Network





The following topics are covered in this section:

- Configuring Internet Protocol Parameters
- Configuring an Access List
- Configuring IPSec
- Configuring a Generic Routing Encapsulation Tunnel Interface
- Configuring the Ethernet Interfaces
- Configuring Static Routes
- Configuration Example

To configure additional features for this network, see Chapter 3, “Feature-by-Feature Router Configurations.”

Configuring Internet Protocol Parameters

Perform the following tasks to configure Internet Protocol (IP) parameters, starting in global configuration mode.

	Command	Task
Step 1	**ip subnet-zero**	Configure the router to recognize the zero subnet range as the valid range of addresses.
Step 2	**no ip finger**	Block incoming IP finger packets.
Step 3	**no ip domain-lookup**	Disable the router from interpreting unfamiliar words (typographical errors) entered during a console session as host names.
Step 4	**ip classless**	Follow classless routing forwarding rules.

Configuring an Access List

Use the **access-list** command to create an access list that permits the GRE protocol, and that specifies the starting and ending IP addresses of the GRE tunnel. Use the following syntax:

access-list 101 permit gre host *ip-address* **host** *ip-address*

In the preceding command line, the first **host** *ip-address* specifies the tunnel starting point, and the second **host** *ip-address* refers to the tunnel end point.

Configuring IPSec

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

	Command	Task
Step 1	**crypto isakmp policy 10**	Define an Internet Key Exchange (IKE) policy, and assign the policy a priority. This command places the router in IKE policy configuration mode.
Step 2	**hash md5**	Specify the md5 hash algorithm for the policy.
Step 3	**authentication pre-share**	Specify pre-share key as the authentication method.
Step 4	**exit**	Exit IKE policy configuration mode.
Step 5	**crypto isakmp key** *name* **address** *ip-address*	Configure a pre-shared key and static IP address for each VPN client.
Step 6	**crypto ipsec transform-set** *name* **esp-des esp-md5-hmac**	Define a combination of security associations to occur during IPSec negotiations.
Step 7	**crypto map** *name* **local-address ethernet 1**	Create a crypto map, and specify and name an identifying interface to be used by the crypto map for IPSec traffic.
Step 8	**crypto map** *name seq-num* **ipsec-isakmp**	Enter crypto map configuration mode, and create a crypto map entry in IPSec ISAKMP mode.
Step 9	**set peer** *ip-address*	Identify the remote IPSec peer.
Step 10	**set transform-set** *name*	Specify the transform set to be used.
Step 11	**match address** *access-list-id*	Specify an extended access list for the crypto map entry.
Step 12	**exit**	Exit crypto map configuration mode.

Configuring a Generic Routing Encapsulation Tunnel Interface

Perform the following tasks to configure generic routing encapsulation (GRE) tunnel interface, starting in global configuration mode.

	Command	Task
Step 1	**interface tunnel 0**	Configure the Tunnel 0 interface.
Step 2	**ip address** *ip-address subnet-mask*	Set the IP address and subnet mask for the Tunnel 0 interface.
Step 3	**tunnel source ethernet 1**	Specify the Ethernet 1 interface as the tunnel source.
Step 4	**tunnel destination** *default-gwy-ip-address*	Specify the default gateway as the tunnel destination.
Step 5	**crypto map** *name*	Associate a configured crypto map to the Tunnel 0 interface.
Step 6	**exit**	Exit Tunnel 0 interface configuration.

Configuring the Ethernet Interfaces

Perform the following tasks to configure the Ethernet 0 and Ethernet 1 interfaces, starting in global configuration mode.

	Command	Task
Step 1	**interface ethernet 0**	Configure the Ethernet 0 interface.
Step 2	**ip address** *ip-address subnet-mask*	Set the IP address and subnet mask for the Ethernet 0 interface.
Step 3	**exit**	Exit Ethernet 0 interface configuration.
Step 4	**interface ethernet 1**	Configure the Ethernet 1 interface.
Step 5	**ip address** *ip-address subnet-mask*	Set the IP address and subnet mask for the Ethernet 1 interface.

	Command	Task
Step 6	**crypto map** *name*	Associate a crypto map with the Ethernet 1 interface.
Step 7	**end**	Exit router configuration mode.

Configuring Static Routes

Perform the following tasks to configure static routes, starting in global configuration mode.

	Command	Task
Step 1	**ip route** *default-gateway-ip-address mask* **ethernet 1**	Create a static route for the Ethernet 1 interface.
Step 2	**ip route** *default-gateway-ip-address mask* **tunnel 0**	Create a static route for the Tunnel 0 interface.
Step 3	**ip route** *default-gateway-ip-address mask gateway-of-last-resort*	Create a static route to the gateway of last resort.
Step 4	**end**	Exit router configuration mode.

Configuration Example

This sample configuration shows IPSec being used over a GRE tunnel.You do not need to enter the commands marked “default.” These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

```
version 12.2
no service single-slot-reload-enable
no service pad (default)
service timestamps debug uptime (default)
service timestamps log uptime (default)
no service password-encryption (default)
!
hostname 806-uut1
!
```

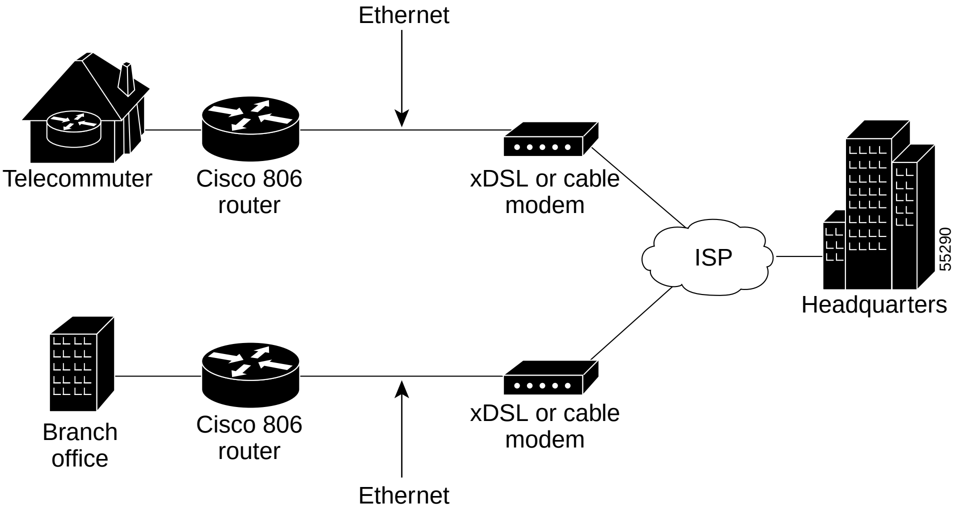
```
logging rate-limit console 10 except errors
no logging console
enable password lab
!
username 3620-1 password 0 testme
ip subnet-zero
no ip finger
no ip domain-lookup
!
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 140.10.10.6
!
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap local-address Ethernet1
crypto map mymap 10 ipsec-isakmp
 set peer 140.10.10.6
 set transform-set myset
 match address 101
!
!
!
interface Tunnel0
 ip address 11.0.0.1 255.0.0.0
 tunnel source Ethernet1
 tunnel destination 140.10.10.6
 crypto map mymap
!
interface Ethernet0
 ip address 192.168.2.100 255.255.255.0
!
interface Ethernet1
 ip address 140.10.10.5 255.255.255.0
 crypto map mymap
!
ip classless (default)
ip route 140.10.10.0 255.255.255.0 Ethernet1
ip route 192.168.1.0 255.255.255.0 Tunnel0
ip route 192.168.1.0 255.255.255.0 140.10.10.6
ip http server (default)
!
access-list 101 permit gre host 140.10.10.5 host 140.10.10.6
!
```

```
line con 0
 exec-timeout 0 0
 transport input none
 stopbits 1
line vty 0 4
 password lab
 login
!
scheduler max-task-time 5000
end
```

Small Office/Telecommuter with Basic Security

Figure 2-2 shows how the Cisco 806 router can be used to provide basic security to users in a small office or to a single telecommuter. The router is either connected to an xDSL modem or to a cable modem that has a connection to an ISP. The router is configured to provide private IP addresses to the devices connected to it, fast switching services, and basic security in the form of access lists and virtual private networking. The router uses Point-to-Point Protocol (PPP) over Ethernet, enabling the computer systems connected to the router to continue to use PPP to connect to the ISP. Private addressing for devices on the premises is provided by network address translation (NAT).

Figure 2-2 Small Office/Telecommuter with Basic Security Configuration



The following topics are covered in this section:

- Configuring the IP Parameters
- Configuring Dynamic Host Configuration Protocol Parameters
- Configuring a Virtual Private Dial-Up Network
- Configuring the Ethernet Interfaces
- Configuring the Dialer Interface
- Configuring the Access List
- Configuration Example

To configure additional features for this network, see Chapter 3, “Feature-by-Feature Router Configurations.”

Configuring the IP Parameters

Perform the following tasks to configure IP parameters, starting in global configuration mode.

	Command	Task
Step 1	**ip subnet-zero**	Configure the router to recognize the zero subnet range as the valid range of addresses.
Step 2	**no ip finger**	Block incoming IP finger packets.
Step 3	**no ip domain-lookup**	Disable the router from interpreting unfamiliar words (typographical errors) entered during a console session as host names.
Step 4	**ip classless**	Follow classless routing forwarding rules.

Configuring Dynamic Host Configuration Protocol Parameters

Perform the following tasks to configure Dynamic Host Configuration Protocol (DHCP), starting 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.
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	**dns-server** *ip-address*	Specify the DNS server.

Configuring a Virtual Private Dial-Up Network

Complete the following tasks to configure a virtual private dial-up network (VPDN), starting 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 mode.
Step 5	**protocol pppoe**	Specify the tunneling protocol as PPPoE.
Step 6	**end**	Exit router configuration mode.

Configuring the Ethernet Interfaces

Configure the Ethernet interfaces by performing the following tasks, starting in global configuration mode.

	Command	Task
Step 1	**interface ethernet 0**	Configure the Ethernet 0 interface.
Step 2	**ip address** *ip-address subnet-mask*	Set the IP address and subnet mask for the Ethernet 0 interface.
Step 3	**ip nat inside**	Establish the Ethernet 0 interface as the inside interface.
Step 4	**ip route-cache**	Enable fast-switching cache for outgoing packets.
Step 5	**ip tcp adjust-mss 1452**	Set the maximum segment size (MSS) of TCP SYN packets. When this command is entered for Ethernet 0, it is automatically added to the Ethernet 1 interface configuration.
Step 6	**exit**	Exit Ethernet 0 interface configuration.
Step 7	**interface ethernet 1**	Configure the Ethernet 1 interface.

	Command	Task
Step 8	**no ip address**	Disable IP addressing for the Ethernet 1 interface.
Step 9	**pppoe enable**	Enable PPPoE as protocol.
Step 10	**pppoe-client dial-pool-number 1**	Create the PPPoE dial pool.
Step 11	**end**	Exit router configuration.

Configuring the Dialer Interface

Complete the following tasks to configure the dialer interface, starting in global configuration mode.

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

Configuring the Access List

The following steps will configure an access list that will enable the user to run any Transmission Control Protocol (TCP) application, but it will block other applications.

Complete the following tasks, starting in global configuration mode.

	Command	Task
Step 1	**ip nat inside source list** *tag* **interface dialer 0 overload**	Configure the NAT parameters for the Dialer 0 interface.
Step 2	**access-list** *tag* **permit ip** *address wildcard-bits*	Configure an access list that permits IP traffic.

Configuration Example

The configuration example that follows shows configurations for DHCP, VPDN, PPPoE, and access lists. Access list configurations in this example will allow TCP applications such as FTP, Telnet, and HTTP.

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

```
!
version 12.2
no service single-slot-reload-enable
no service pad (default)
service timestamps debug uptime (default)
service timestamps log uptime (default)
no service password-encryption (default)
!
hostname router1
!
no logging buffered
logging rate-limit console 10 except errors
!
ip subnet-zero
no ip finger
no ip domain-lookup
!
!
```

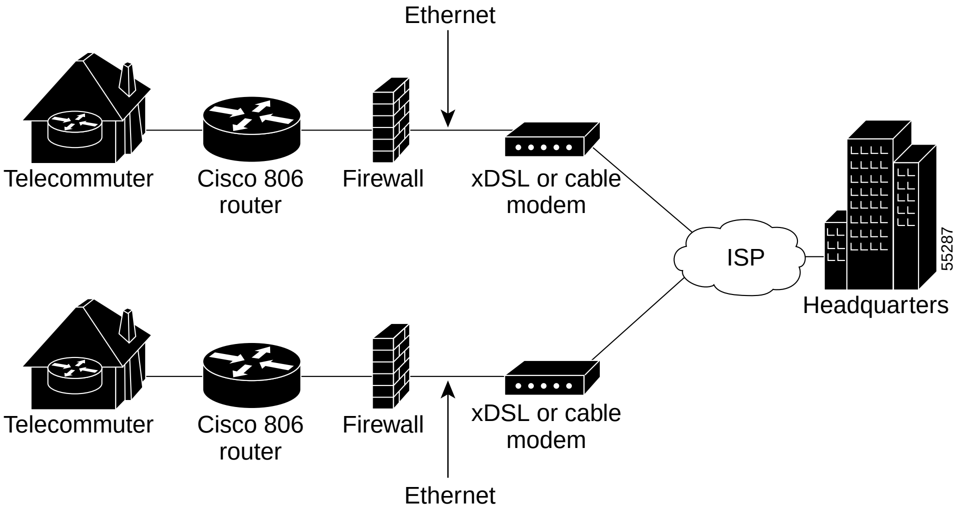
```
ip dhcp excluded-address 192.168.1.1
dhcp pool PrivateNet
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 dns-server 140.10.10.1
!
!
no ip dhcp-client network-discovery
vpdn enable
!
vpdn-group 1
 request-dialin
  protocol pppoe
!
!
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
 ip tcp adjust-mss 1452 (required for router to reach all websites)
 ip nat inside
 ip route-cache
!
!
interface Ethernet1
 no ip address
 ip tcp adjust-mss 1452
 pppoe enable
 pppoe-client dial-pool-number 1
!
!
interface Dialer0
 ip address 140.10.10.5 255.255.255.0
 ip nat outside
 ip mtu 1492
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 ppp authentication chap
!
ip classless
! ACL For Nat
access-list 101 permit ip 192.168.1.0 0.255.255.255 any
ip nat inside source list 101 interface Dialer0 overload
ip route 0.0.0.0 0.0.0.0 Dialer0
ip http server
!
!
```

```
line con 0
 exec-timeout 0 0
 transport input none
 stopbits 1
line vty 0 4
login
!
scheduler max-task-time 5000
end
```

Small Office/Telecommuter with Business-Class Security

Figure 2-3 shows how the Cisco 806 router can be used to provide business-class security to a small office or to a telecommuter. Besides configuring the security features described in the "Small Office/Telecommuter with Basic Security" section on page 2-8, the network administrator has configured the router to inspect the application-layer protocols of the packets that arrive. The Cisco 806 router is connected either to a DSL modem or to a cable modem in this configuration. The router uses PPPoE and private addressing provided by NAT.

Figure 2-3 Business Class Security Configuration



This section includes the following topics:

- Configuring the IP Parameters
- Configuring DHCP
- Configuring a Set of Inspection Rules
- Configuring a VPDN
- Configuring the Ethernet Interfaces
- Configuring the Dialer Interface
- Configuring the Access List
- Configuration Example

To configure additional features for this network, see Chapter 3, "Feature-by-Feature Router Configurations."

Configuring the IP Parameters

Perform the following tasks to configure the IP parameters, starting in global configuration mode.

	Command	Task
Step 1	**ip subnet-zero**	Configure the router to recognize the zero subnet range as the valid range of addresses.
Step 2	**no ip finger**	Block incoming IP finger packets.
Step 3	**no ip domain-lookup**	Disable the router from interpreting unfamiliar words (typographical errors) entered during a console session as host names.
Step 4	**ip classless**	Follow classless routing forwarding rules.

Configuring DHCP

Perform the following tasks to configure DHCP, starting 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.
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	**dns-server** *ip-address*	Specify the DNS server.

Configuring a Set of Inspection Rules

Specify which protocols to examine by using the **ip inspect name** command. 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 that can be referenced elsewhere in the configuration.

Configuring a VPDN

Complete the following tasks to configure a VPDN, starting 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 mode.
Step 5	**protocol pppoe**	Specify the tunneling protocol as PPPoE.
Step 6	**end**	Exit router configuration mode.

Configuring the Ethernet Interfaces

Configure the Ethernet interfaces by performing the following tasks, starting in global configuration mode.

	Command	Task
Step 1	**interface ethernet 0**	Configure the Ethernet 0 interface.
Step 2	**ip address** *ip-address subnet-mask*	Set the IP address and subnet mask for the Ethernet 0 interface.

	Command	Task
Step 3	**ip nat inside**	Establish the Ethernet 0 interface as the inside interface.
Step 4	**ip route-cache**	Enable fast-switching cache for outgoing packets.
Step 5	**ip tcp adjust-mss 1452**	Set the maximum segment size (MSS) of TCP SYN packets. When this command is entered for Ethernet 0, it is automatically added to the Ethernet 1 interface configuration.
Step 6	**exit**	Exit Ethernet 0 interface configuration.
Step 7	**interface ethernet 1**	Configure the Ethernet 1 interface.
Step 8	**no ip address**	Disable IP addressing for the Ethernet 1 interface.
Step 9	**pppoe enable**	Enable PPPoE as protocol.
Step 10	**pppoe-client dial-pool-number 1**	Create the PPPoE dial pool.
Step 11	**end**	Exit router configuration.

Configuring the Dialer Interface

Complete the following tasks to configure the dialer interface, starting in global configuration mode.

	Command	Task
Step 1	**ip route** *default-gateway-ip-address mask* **dialer 0**	For the Dialer 0 interface, set the IP route for the default gateway.
Step 2	**interface dialer 0**	Enter Dialer 0 interface configuration.
Step 3	**ip address** *ip-address subnet-mask*	Specify the IP address and subnet mask for the Dialer 0 interface.
Step 4	**ip mtu 1492**	Set the size of the IP maximum transmission unit (MTU).
Step 5	**ip nat outside**	Establish the Dialer 0 interface as the outside interface.

	Command	Task
Step 6	**encapsulation ppp**	Set the encapsulation type to PPP.
Step 7	**dialer pool 1**	Specify the dialer pool to be used.
Step 8	**ppp authentication pap callin**	Set the PPP link authentication method to Password Authentication Protocol (PAP), and specify that remote network nodes are to be authenticated on callin only.
Step 9	**ppp pap sent-username** *name* **password** *password*	Set the PAP authentication parameters.
Step 10	**dialer-group 1**	Assign this interface to a dialer list.
Step 11	**ppp authentication chap**	Set the PPP authentication method to Challenge Handshake Authentication Protocol (CHAP).
Step 12	**ip access-group** *tag* **in**	Specify an access list to apply to inbound packets.
Step 13	**ip inspect** *name* **in**	Specify the set of inspection criteria to apply to inbound packets.
Step 14	**ip route-cache**	Enable fast-switching cache for outgoing packets.
Step 15	**exit**	Exit Dialer 0 interface configuration.

Configuring the Access List

The following configuration steps will configure a firewall that will allow TCP sessions originating from the local area network (LAN), but will block all TCP sessions that originate on the wide area network (WAN).

Complete the following tasks, starting in global configuration mode.

	Command	Task
Step 1	**ip nat inside source list** *tag* **interface dialer 0 overload**	Configure the NAT parameters for the Dialer 0 interface.
Step 2	**access-list** *tag* **deny ip host 255.255.255.255 any**	Configure an access list that blocks all traffic originating outside the firewall.

	Command	Task
Step 3	**access-list** *tag* **deny ip ip-address 0.0.0.255** any	Configure an access list that prevents spoofing.
Step 4	**access-list** *tag* **permit icmp any any** *message-type*	Allow Internet Control Message Protocol (ICMP) messages of the specified type to be exchanged.

Configuration Example

The Dialer 0 interface is the WAN interface. Therefore, all access lists and inspect lists are applied to that interface. The firewall configured in this example will allow TCP and User Datagram Protocol (UDP) connections that originate inside the firewall. However, any connection that originates outside the firewall would be blocked, except for certain types of ICMP packets.

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

```
version 12.2
no service single-slot-reload-enable
no service pad (default)
service timestamps debug uptime (default)
service timestamps log uptime (default)
no service password-encryption (default)
!
hostname router1
!
no logging buffered
logging rate-limit console 10 except errors
!
ip subnet-zero
no ip finger
no ip domain-lookup
!
!
ip dhcp excluded-address 192.168.1.1
dhcp pool PrivateNet
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 dns-server 140.10.10.1
!
ip inspect name myfw tcp alert on
ip inspect name myfw cuseeme timeout 3600
ip inspect name myfw ftp timeout 3600
ip inspect name myfw http timeout 3600
ip inspect name myfw rcmd timeout 3600
ip inspect name myfw realaudio timeout 3600
ip inspect name myfw smtp timeout 3600
ip inspect name myfw tftp timeout 30
ip inspect name myfw udp timeout 15
ip inspect name myfw tcp timeout 3600
ip inspect name myfw h323 timeout 3600
!
!
vpdn enable
!
vpdn-group 1
 request-dialin
  protocol pppoe
!
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
 ip tcp adjust-mss 1452 (required for router to reach all websites)
 ip nat inside
 ip route-cache
!
!
interface Ethernet1
 no ip address
 ip tcp adjust-mss 1452
 pppoe enable
 pppoe-client dial-pool-number 1
!
!
interface Dialer0
 ip address 140.10.10.5 255.255.255.0
 ip nat outside
 ip inspect myfw out
 ip access-group 105 in
 ip mtu 1492
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 ppp authentication chap
!
ip classless
!for blocking all traffic originating from outside premises
access-list 105 deny ip host 255.255.255.255 any
!Done for antispoofing
access-list 105 deny ip 192.168.1.0 0.0.0.255 any
```

```
!
!done to permit administrative ICMP messages
!
!
access-list 105 permit icmp any any echo-reply
access-list 105 permit icmp any any time-exceeded
access-list 105 permit icmp any any packet-too-big
access-list 105 permit icmp any any traceroute
access-list 105 permit icmp any any unreachable
!
```

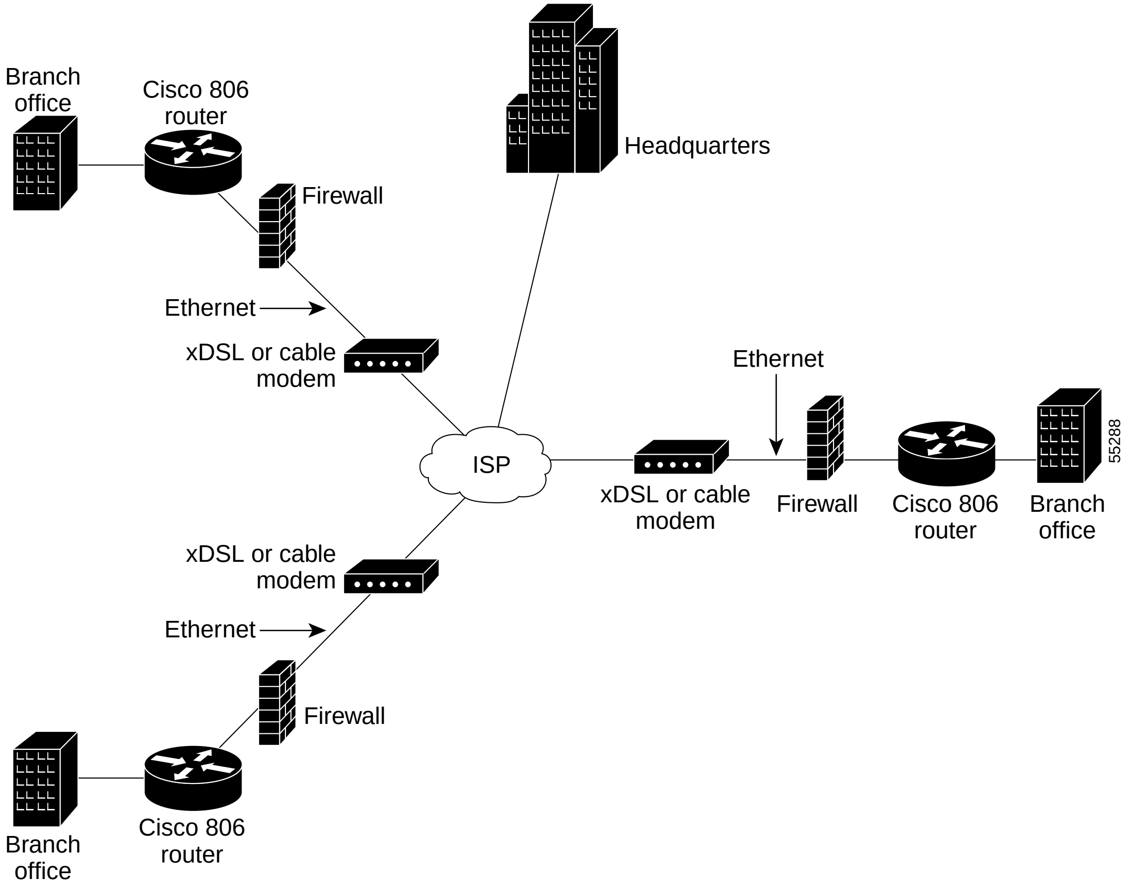
```
! ACL For Nat
access-list 101 permit ip 192.168.1.0 0.255.255.255 any
ip nat inside source list 101 interface Dialer0 overload
ip route 0.0.0.0 0.0.0.0 Dialer0
ip http server
!
!
line con 0
 exec-timeout 0 0
 transport input none
 stopbits 1
line vty 0 4
login
!
scheduler max-task-time 5000
end
!
```

Small Office/Telecommuter with Business-Class Security and Enterprise Applications

This scenario includes the business-class security features described in Small Office/Telecommuter with Business-Class Security, page 2-15, and includes support for enterprise applications such as NetMeeting. It also supports multicasting, which enables users at the premises to share a single data stream to the Cisco 806 router for things like video-on-demand presentations and video conferencing, thus conserving network bandwidth.

Figure 2-4 shows three branch offices linked to a headquarters office using xDSL modems or cable modems that connect to an ISP.

Figure 2-4 Business-Class Security and Enterprise Applications Configuration



This section includes the following topics:

- Configuring the IP Parameters
- Configuring Multicast Routing
- Configuring DHCP
- Configuring a Set of Inspection Rules
- Configuring a VPDN
- Configuring the Ethernet Interfaces

- Configuring the Dialer Interface
- Configuring the Access List
- Configuration Example

To configure additional features for this network, see Chapter 3, “Feature-by-Feature Router Configurations.”

Configuring the IP Parameters

Perform the following tasks to configure the IP parameters, starting in global configuration mode.

	Command	Task
Step 1	**ip subnet-zero**	Configure the router to recognize the zero subnet range as the valid range of addresses.
Step 2	**no ip finger**	Block incoming IP finger packets.
Step 3	**no ip domain-lookup**	Disable the router from interpreting unfamiliar words (typographical errors) entered during a console session as host names.
Step 4	**ip classless**	Follow classless routing forwarding rules.

Configuring Multicast Routing

Configure multicast routing by completing the following tasks, starting in global configuration mode.

	Command	Task
Step 1	**ip multicast-routing**	Enable IP multicast forwarding.
Step 2	**ip pim rp-address** *address*	Configure the Protocol Independent Multicasting (PIM) Rendezvous Point (RP) address.

Configuring DHCP

Configure DHCP by completing the following tasks, starting 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.
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	**dns-server** *ip-address*	Specify the DNS server.

Configuring a Set of Inspection Rules

Specify which protocols to examine by using the **ip inspect name** command. 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 that can be referenced elsewhere in the configuration.

Configuring a VPDN

Complete the following tasks to configure a VPDN, starting 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 mode.
Step 5	**protocol pppoe**	Specify the tunneling protocol as PPPoE.
Step 6	**end**	Exit router configuration mode.

Configuring the Ethernet Interfaces

Configure the Ethernet interfaces by performing the following tasks, starting in global configuration mode.

	Command	Task
Step 1	**interface ethernet 0**	Configure the Ethernet 0 interface.
Step 2	**ip address** *ip-address subnet-mask*	Set the IP address and subnet mask for the Ethernet 0 interface.
Step 3	**ip nat inside**	Establish the Ethernet 0 interface as the inside interface.
Step 4	**ip pim sparse-mode**	Enable PIM sparse-mode operation.
Step 5	**ip route-cache**	Enable fast-switching cache for outgoing packets.
Step 6	**ip tcp adjust-mss 1452**	Set the maximum segment size (MSS) of TCP SYN packets. When this command is entered for Ethernet 0, it is automatically added to the Ethernet 1 interface configuration.
Step 7	**exit**	Exit Ethernet 0 interface configuration.

	Command	Task
Step 8	**interface ethernet 1**	Configure the Ethernet 1 interface.
Step 9	**no ip address**	Disable IP addressing for the Ethernet 1 interface.
Step 10	**pppoe enable**	Enable PPPoE as the protocol.
Step 11	**pppoe-client dial-pool-number** *tag*	Create a PPPoE dial pool.
Step 12	**end**	Exit router configuration.

Configuring the Dialer Interface

Complete the following tasks to configure the dialer interface, starting in global configuration mode.

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

	Command	Task
Step 10	**ppp authentication pap callin**	Set the PPP link authentication method to Password Authentication Protocol (PAP), and specify that remote network nodes are to be authenticated on callin only.
Step 11	**ppp pap sent-username** *name* **password** *password*	Set the PAP authentication parameters.
Step 12	**ip access-group** *tag* **in**	Specify a configured access list to apply to inbound packets.
Step 13	**ip inspect** *name* **in**	Specify the set of inspection criteria to apply to inbound packets.
Step 14	**ip pim sparse-mode**	Enable PIM sparse-mode operation.
Step 15	**ip route-cache**	Enable fast-switching cache for outgoing packets.
Step 16	**exit**	Exit Dialer 0 interface configuration.

Configuring the Access List

Complete the following configuration steps to configure a firewall that will allow TCP sessions originating from the local area network (LAN), but will block all TCP sessions that originate on the wide area network (WAN).

Complete the following tasks, starting in global configuration mode.

	Command	Task
Step 1	**ip nat inside source list** *tag* **interface dialer 0 overload**	Configure the NAT parameters for the Dialer 0 interface.
Step 2	**access-list** *tag* **deny ip host 255.255.255.255 any**	Configure an access list that blocks all traffic originating outside the firewall.
Step 3	**access-list** *tag* **deny ip ip-address 0.0.0.255** any	Configure an access list that prevents spoofing.
Step 4	**access-list** *tag* **permit icmp any any** *message-type*	Allow Internet Control Message Protocol (ICMP) messages of the specified type to be exchanged.

Configuration Example

The configuration example that follows shows configurations for DHCP, VPDN, PPPoE, IP multicasting, and firewalls. The firewalls configured in this example will allow TCP and UDP connections that originate from the premises. However, any connection that originates outside the firewall would be blocked. Access list configurations will allow TCP applications such as FTP, Telnet, and HTTP, while blocking raw IP packets.

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

Note Multicasting is configured in PIM sparse mode. The user must change the IP address of the RP server manually.

```
!
version 12.2
no service single-slot-reload-enable
no service pad (default)
service timestamps debug uptime (default)
service timestamps log uptime (default)
no service password-encryption (default)
!
hostname router1
!
no logging buffered
logging rate-limit console 10 except errors
!
ip subnet-zero
no ip finger
no ip domain-lookup
!
!
ip dhcp excluded-address 192.168.1.1
dhcp pool PrivateNet
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
dns-server 140.10.10.1
!
!Multicast Protocol - PIM
ip multicast-routing
ip pim rp-address 192.168.20.3
```

```
!
ip inspect name myfirewall tcp alert on
ip inspect name myfw cuseeme timeout 3600
ip inspect name myfw ftp timeout 3600
ip inspect name myfw http timeout 3600
ip inspect name myfw rcmd timeout 3600
ip inspect name myfw realaudio timeout 3600
ip inspect name myfw smtp timeout 3600
ip inspect name myfw tftp timeout 30
ip inspect name myfw udp timeout 15
ip inspect name myfw tcp timeout 3600
ip inspect name myfw h323 timeout 3600
!
!
no ip dhcp-client network-discovery
vpdn enable
!
vpdn-group 1
 request-dialin
  protocol pppoe
!
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
 ip pim sparse-mode
 ip tcp adjust-mss 1452 (required for router to reach all websites)
 ip nat inside
!
!
interface Ethernet1
 no ip address
 ip tcp adjust-mss 1452
 pppoe enable
 pppoe-client dial-pool-number 1
!
!
interface Dialer0
 ip address 140.10.10.5 255.255.255.0
 ip pim sparse-mode
 ip access-group 102 out
 ip nat outside
 ip inspect myfw out
 ip access-group 105 in
 ip mtu 1492
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 ppp authentication chap
 ip route-cache
```

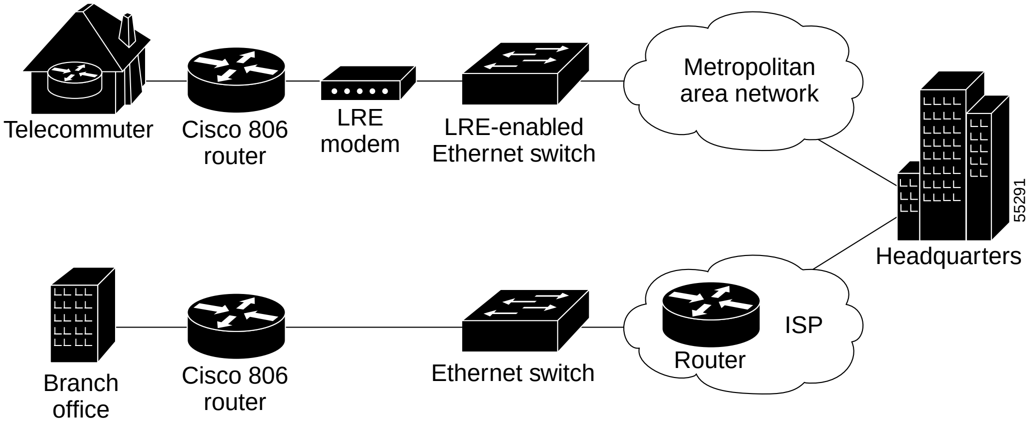
```
!
ip classless
!for blocking all traffic originating from outside premises
access-list 105 deny ip host 255.255.255.255 any
!Done for antispoofing
access-list 105 deny ip 192.168.1.0 0.0.0.255 any
!
!done to permit administrative ICMP messages
!
!
access-list 105 permit icmp any any echo-reply
access-list 105 permit icmp any any time-exceeded
access-list 105 permit icmp any any packet-too-big
access-list 105 permit icmp any any traceroute
access-list 105 permit icmp any any unreachable
!
! ACL For Nat
access-list 101 permit ip 192.168.1.0 0.255.255.255 any
ip nat inside source list 101 interface Dialer0 overload
ip route 0.0.0.0 0.0.0.0 Dialer0
ip http server
!
!
line con 0
 exec-timeout 0 0
 transport input none
 stopbits 1
line vty 0 4
login
!
scheduler max-task-time 5000
end

!
```

Ethernet Gateway

The configuration for this scenario is identical to the configuration described in the “Small Office/Telecommuter with Business-Class Security and Enterprise Applications” section on page 2-23. In this case, however, the Cisco 806 router connects to a long-reach Ethernet (LRE) modem or to an Ethernet switch, as shown in Figure 2-5 on page 2-33. Remote offices and telecommuters can be carried by a metropolitan area network (MAN), or an ISPs network.

Figure 2-5 Ethernet Gateway Configuration



See the “Small Office/Telecommuter with Business-Class Security and Enterprise Applications” section on page 2-23 for configuration instructions and a configuration example.

This section includes The following topics:

- Configuring the IP Parameters
- Configuring Multicast Routing
- Configuring DHCP
- Configuring a Set of Inspection Rules
- Configuring a VPDN
- Configuring the Ethernet Interfaces
- Configuring the Dialer Interface
- Configuring the Access List
- Configuration Example

To configure additional features for this network, see Chapter 3, “Feature-by-Feature Router Configurations.”

Configuring the IP Parameters

Perform the following tasks to configure the IP parameters, starting in global configuration mode.

	Command	Task
Step 1	**ip subnet-zero**	Configure the router to recognize the zero subnet range as the valid range of addresses.
Step 2	**no ip finger**	Block incoming IP finger packets.
Step 3	**no ip domain-lookup**	Disable the router from translating unfamiliar words (typographical errors) entered during a console session into IP addresses.
Step 4	**ip classless**	Follow classless routing forwarding rules.

Configuring Multicast Routing

Complete the following tasks to configure multicast routing, starting in global configuration mode.

	Command	Task
Step 1	**ip multicast routing**	Enable IP-multicast forwarding.
Step 2	**ip pim rp-address** *address*	Specify a PIM RP address.

Configuring DHCP

Configure DHCP by completing the following tasks, starting 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.
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 name of the default router.
Step 5	**dns-server** *ip-address*	Specify the DNS server.

Configuring a Set of Inspection Rules

Specify which protocols to examine by using the **ip inspect name** command. 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 that can be referenced elsewhere in the configuration.

Configuring a VPDN

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

	Command	Task
Step 5	**protocol pppoe**	Specify the tunneling protocol as PPPoE.
Step 6	**end**	Exit router configuration mode.

Configuring the Ethernet Interfaces

Configure the Ethernet interfaces by performing the following tasks, starting in global configuration mode.

	Command	Task
Step 1	**interface ethernet 0**	Configure the Ethernet0 interface.
Step 2	**ip address** *ip-address subnet-mask*	Set the IP address and subnet mask for the Ethernet0 interface.
Step 3	**ip nat inside**	Establish the Ethernet0 interface as the inside interface.
Step 4	**ip pim sparse-mode**	Enable PIM sparse-mode operation.
Step 5	**ip route-cache**	Enable fast-switching cache for outgoing packets.
Step 6	**ip adjust-mss 1452**	Set the maximum segment size of TCP SYN packets.
Step 7	**exit**	Exit Ethernet0 interface configuration.
Step 8	**interface ethernet 1**	Configure the Ethernet1 interface.
Step 9	**no ip address**	Disable IP addressing for the Ethernet1 interface.
Step 10	**pppoe enable**	Enable PPPoE as the protocol.
Step 11	**ppoe-client dial-pool-number** *tag*	Create a PPPoE dial pool.
Step 12	**end**	Exit router configuration.

Configuring the Dialer Interface

Complete the following tasks to configure the dialer interface, starting in global configuration mode.

	Command	Task
Step 1	**ip route** *default-gateway-ip-address mask* **dialer 0**	For the Dialer0 interface, set the IP route for the default gateway.
Step 2	**interface dialer 0**	Enter Dialer0 interface configuration.
Step 3	**ip address negotiated**	Specify that the IP address is to be negotiated over PPP.
Step 4	**ip mtu 1492**	Set the size of the IP maximum transmission unit (MTU).
Step 5	**ip nat outside**	Establish the Dialer0 interface as the outside interface.
Step 6	**encapsulation ppp**	Set the encapsulation type to PPP.
Step 7	**dialer pool 1**	Specify the dialer pool to be used.
Step 8	**ppp authentication pap callin**	Set the PPP link authentication method to Password Authentication Protocol (PAP), and specify that remote network nodes are to be authenticated on callin only.
Step 9	**ppp pap sent-username** *name* **password** *password*	Set the PAP authentication parameters.
Step 10	**dialer-group 1**	Assign this interface to a dialer list.
Step 11	**ppp authentication chap**	Set the PPP authentication method to Challenge Handshake Authentication Protocol (CHAP).
Step 12	**ip access-group** *tag* **in**	Specify an access list to apply to inbound packets.
Step 13	**ip inspect** *name* **in**	Specify the set of inspection criteria to apply to inbound packets.
Step 14	**ip pim sparse-mode**	Enable PIM sparse-mode operation.

	Command	Task
Step 15	**ip route-cache**	Enable fast-switching cache for outgoing packets.
Step 16	**exit**	Exit Dialer0 interface configuration.

Configuring the Access List

The following configuration steps will configure a firewall that will allow TCP sessions originating from the local area network (LAN), but will block all TCP sessions that originate on the wide area network (WAN).

Complete the following tasks, starting in global configuration mode.

	Command	Task
Step 1	**ip nat inside source list** *tag* **interface dialer 0 overload**	Configure the NAT parameters for the Dialer0 interface.
Step 2	**access-list** *tag* **permit** *address wildcard-bits* **log**	Configure an access list that logs matches to the address and wildcard bits.
Step 3	**access-list** *tag* **deny ip any any**	Deny IP traffic from any source host or to any destination host.

Configuration Example

The configuration example that follows shows configurations for DHCP, VPDN, PPPoE, IP multicasting and firewalls. The firewalls configured in this example will allow TCP and UDP connections that originate from the premises. However, any connection that originates outside the firewall would be blocked. Access list configurations will allow TCP applications such as FTP, Telnet, and HTTP, while blocking raw IP packets.

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

Note IP multicasting is configured in PIM sparse mode. The user must change the IP address of the RP server manually.

```
!
version 12.2
no service single-slot-reload-enable
no service pad (default)
service timestamps debug uptime (default)
service timestamps log uptime (default)
no service password-encryption (default)
!
hostname router1
!
no logging buffered
logging rate-limit console 10 except errors
!
ip subnet-zero
no ip finger
no ip domain-lookup
!
!
ip dhcp excluded-address 192.168.1.1
dhcp pool PrivateNet
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
dns-server 140.10.10.1
!
!Multicast Protocol - PIM
ip multicast-routing
ip pim rp-address 192.168.20.3

!
ip inspect name myfirewall tcp alert on
ip inspect name myfw cuseeme timeout 3600
ip inspect name myfw ftp timeout 3600
ip inspect name myfw http timeout 3600
ip inspect name myfw rcmd timeout 3600
ip inspect name myfw realaudio timeout 3600
ip inspect name myfw smtp timeout 3600
ip inspect name myfw tftp timeout 30
ip inspect name myfw udp timeout 15
ip inspect name myfw tcp timeout 3600
ip inspect name myfw h323 timeout 3600
!
!
no ip dhcp-client network-discovery
```

```
vpdn enable
!
vpdn-group 1
 request-dialin
  protocol pppoe
!
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
 ip pim sparse-mode
 ip adjust-mss 1452
 ip nat inside
 ip route-cache
!
!
interface Ethernet1
 no ip address
 ip adjust-mss 1452
 pppoe enable
 pppoe-client dial-pool-number 1
!
!
interface Dialer0
 ip address 140.10.10.5 255.255.255.0
 ip pim sparse-mode
 ip access-group 102 out
 ip nat outside
 ip inspect myfw out
 ip access-group 105 in
 ip mtu 1492
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 ppp authentication chap
 ip route-cache
!
ip classless
!for blocking all traffic originating from outside premises
access-list 105 deny ip host 255.255.255.255 any
!Done for antispoofing
access-list 105 deny ip 192.168.1.0 0.0.0.255 any
!
!done to permit administrative ICMP messages
!
!
access-list 105 permit icmp any any echo-reply
access-list 105 permit icmp any any time-exceeded
access-list 105 permit icmp any any packet-too-big
access-list 105 permit icmp any any traceroute
```

```
access-list 105 permit icmp any any unreachable
!
! ACL For Nat
access-list 101 permit ip 192.168.1.0 0.255.255.255 any
ip nat inside source list 101 interface Dialer0 overload
ip route 0.0.0.0 0.0.0.0 Dialer0
ip http server
!
!
line con 0
 exec-timeout 0 0
 transport input none
 stopbits 1
line vty 0 4
login
!
scheduler max-task-time 5000
end
!
```

Feature-by-Feature Router Configurations

This chapter includes feature-by-feature configuration procedures for the Cisco 806 router. This chapter is useful if you have a network in place and you want to add specific features.

If you prefer to use network scenarios to build a network, see Chapter 2, “Network Scenarios.”

This chapter contains the following sections:

- Before You Configure Your Network
- Configuring Basic Parameters
- Configuring Bridging
- Configuring Routing
- Configuring PPPoE Support
- Configuring Network Address Translation
- Configuring Dynamic Host Configuration Protocol
- Configuring IP Multicasting
- Configuring an Extended Access List
- Configuring Network Time Protocol Support
- Configuring IP Security and Generic Routing Encapsulation Tunneling
- Configuring Other Security Features
- Configuring Service Assurance Agent Support

Note When you configure Ethernet interfaces, be aware that Ethernet 0 is the interface for hubbed ETHERNET ports 1 through 4, which support the local area network (LAN) on the premises, and Ethernet 1 is the interface for the INTERNET ETHERNET port.

Before You Configure Your Network

Before you configure your network, you must do the following:

- Arrange for a digital subscriber line (DSL), cable, or Ethernet connection with your service provider.
- If you are setting up an Internet connection, gather the following information:
  - Point-to-Point Protocol (PPP) client name that is assigned as your login name
  - PPP authentication type—Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP)
  - PPP password for accessing your Internet service provider (ISP) account
  - Domain Name System (DNS) server IP address and default gateways
- If you are setting up a connection to a corporate network, you and its network administrator must generate and share the following information for the WAN interfaces of the routers:
  - PPP authentication type—CHAP or PAP
  - PPP client name for accessing the router
  - PPP password for accessing the router
- If you are setting up Internet Protocol (IP) routing, generate the addressing scheme for your IP network.

Configuring Basic Parameters

To configure the router, perform the tasks described in the following sections:

- Configuring Global Parameters
- Configuring the Ethernet Interfaces
- Configuring a Console Line for the Router

After your router boots, the following prompt displays. Enter **no**.

```
Would you like to enter the initial configuration dialog [yes]: no
```

For complete information on how to access global configuration mode, see the "Entering Global Configuration Mode" section in Appendix A, "Cisco IOS Basic Skills."

Configuring Global Parameters

Perform the following steps to configure the router for global parameters:

	Command	Task
Step 1	**configure terminal**	Enter configuration mode.
Step 2	**hostname** *name*	Specify the name for the router.
Step 3	**enable secret** *password*	Specify an encrypted password to prevent unauthorized access to the router.
Step 4	**ip subnet-zero**	Configure the router to recognize the zero subnet range as the valid range of addresses.
Step 5	**no ip domain-lookup**	Disable the router from interpreting unfamiliar words (typographical errors) entered during a console session as host names.

For complete information on the global parameter commands, refer to the Cisco IOS Release 12.0 documentation set.

Configuring the Ethernet Interfaces

To configure the Ethernet interfaces, perform the following steps, beginning in global configuration mode.

	Command	Task
Step 1	**interface ethernet 0**	Enter configuration mode for the Ethernet 0 interface.
Step 2	**ip address** *ip-address mask*	Set the IP address and subnet mask for the Ethernet 0 interface.
Step 3	**no shutdown**	Enable the Ethernet 0 interface to change the state from administratively down to up.
Step 4	**exit**	Exit configuration mode for the Ethernet 0 interface.
Step 5	**interface ethernet 1**	Enter configuration mode for the Ethernet 1 interface.
Step 6	**ip address** *ip-address mask*	Set the IP address and subnet mask for the Ethernet 1 interface.
Step 7	**no shutdown**	Enable the Ethernet 1 interface to change the state from administratively down to up.
Step 8	**end**	Exit router configuration mode.

For complete information on the Ethernet commands, refer to the Cisco IOS Release 12.0 documentation set. For more general information on Ethernet concepts, see Chapter 1, “Concepts.”

Configuration Example

The following example shows the Ethernet interface configuration. You do not need to enter the commands marked “default.” These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

```
!
interface Ethernet0
ip address 192.168.1.1 255.255.255.0
```

```
no ip directed-broadcast (default)
!
interface Ethernet1
ip address 192.168.2.1 255.255.255.0
no ip directed-broadcast (default)
!
```

Verifying Your Configuration

To verify that you have properly configured the Ethernet interface, enter the **show interface ethernet 0** command and the **show interface ethernet 1** command. You should see a verification output like the following examples:

```
router#show interface ethernet 0
Ethernet0 is up, line protocol is up
  Hardware is PQUICC Ethernet, address is 00ff.ff20.008e
  (bia 00ff.ff20.008e)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)

router#show interface ethernet 1
Ethernet1 is up, line protocol is up
  Hardware is PQUICC_FEC, address is 00ff.ff20.008f
  (bia 00ff.ff20.008f)
  Internet address is 192.168.2.1/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
```

Configuring a Console Line for the Router

To configure a console line that you can use to access the router over the network, perform the following steps, beginning in global configuration mode.

	Command	Task
Step 1	**line console 0**	Enter line configuration mode, and specify the console terminal line.
Step 2	**password** *password*	Specify a unique password on the line.
Step 3	**login**	Enable password checking at terminal session login.
Step 4	**exec-timeout 10 0**	Set the interval that EXEC command interpreter waits until user input is detected. Exec-timeout 10 0 is the default.
Step 5	**line vty 0 4**	Specify a virtual terminal for remote console access.
Step 6	**transport input ssh**	This step is optional. Specify that only Secure Shell (SSH) be used for interactive logins to the router.
Step 7	**password** *password*	Specify a unique password on the line.
Step 8	**login**	Enable password checking at virtual terminal session login.
Step 9	**end**	Exit line configuration mode, and return to privileged EXEC mode.

For complete information on the command line commands, refer to the Cisco IOS Release 12.0 documentation set.

Configuration Example

The following configuration shows the command-line access commands.

You do not need to input the commands marked “default.” These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

```
!
line con 0
exec-timeout 10 0
password 4youreyesonly
login
transport input none (default)
stopbits 1 (default)
line vty 0 4
password secret
login
!
```

Verifying Your Configuration

You can verify your configuration by entering the **show line console 0** command. The following example shows partial output from this command.

```
router#show line console 0
   Tty Typ     Tx/Rx    A Modem  Roty AccO AccI   Uses   Noise
Overruns   Int
*    0 CTY             -    -      -    -    -      0      1     0/0
-

Line 0, Location: "", Type: ""
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 9600/9600, no parity, 1 stopbits, 8 databits...
```

Configuring Bridging

Bridges are store-and-forward devices that use unique hardware addresses to filter traffic that would otherwise travel from one segment to another. You can configure the Cisco 806 router as a pure bridge.

To configure bridging, perform the following steps, beginning in global configuration mode.

	Command	Task
Step 1	**no ip routing**	Disable IP routing.
Step 2	**bridge** *number* **protocol** *protocol*	Specify the bridge protocol to define the type of Spanning-Tree Protocol (STP).

	Command	Task
Step 3	**interface ethernet 0**	Enter configuration mode for the Ethernet 0 interface.
Step 4	**bridge-group** *number*	Specify the bridge-group number to which the Ethernet 0 interface belongs.
Step 5	**no shutdown**	Enable the Ethernet 0 interface.
Step 6	**exit**	Exit configuration mode for the Ethernet 0 interface.
Step 7	**interface ethernet 1**	Enter configuration mode for the Ethernet 1 interface.
Step 8	**bridge-group** *number*	Specify the bridge-group number to which the Ethernet 1 interface belongs.
Step 9	**no shutdown**	Enable the Ethernet 1 interface.
Step 10	**end**	Exit router configuration mode.

For complete information on the bridging commands, refer to the Cisco IOS Release 12.0 documentation set. For more general concepts on bridging, see Chapter 1, “Concepts.”

Configuration Example

The following configuration example uses bridging. You do not need to enter the commands marked “default.” These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

This configuration example shows the Ethernet 0 and Ethernet 1 interfaces configured. The Ethernet interface has IP addressing turned off for bridging, and IP-directed broadcast is disabled, which prevents the translation of directed broadcasts to physical broadcasts. The bridge-group number with which the Ethernet 1 interface is associated is set to 1. The bridge protocol is set to 1 to define the STP.

```
no ip routing
!
interface Ethernet0
no ip address
no ip directed-broadcast (default)
```

```
bridge-group 1
!
interface Ethernet1
no ip address
no ip directed-broadcast (default)
bridge-group 1
!
ip classless (default)
!
bridge 1 protocol ieee
!
end
```

Verifying Your Configuration

To verify that you have properly configured bridging, enter the **show spanning-tree** command. You should see a verification output similar to the following example:

```
router#show spanning-tree

Bridge group 1 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, address 00ff.ff20.008e
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32768, address 00d0.d373.2ec0
  Root port is 2 (Ethernet0), cost of root path is 200
  Topology change flag not set, detected flag not set
  Number of topology changes 1 last change occurred 00:00:38 ago
          from Ethernet0
  Times: hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers:hello 0, topology change 0, notification 0, aging 300

 Port 2 (Ethernet0) of Bridge group 1 is forwarding
   Port path cost 100, Port priority 128, Port Identifier 128.2.
   Designated root has priority 32768, address 00d0.d373.2ec0
   Designated bridge has priority 32768, address 00e0.1e58.8af2
   Designated port id is 128.4, designated path cost 100
   Timers:message age 2, forward delay 0, hold 0
   Number of transitions to forwarding state:1
   BPDU:sent 1, received 35

 Port 3 (Ethernet1) of Bridge group 1 is forwarding
   Port path cost 100, Port priority 128, Port Identifier 128.3.
   Designated root has priority 32768, address 00d0.d373.2ec0
   Designated bridge has priority 32768, address 00ff.ff20.008e
   Designated port id is 128.3, designated path cost 200
   Timers:message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state:1
   BPDU:sent 26, received 0

router#
```

Configuring Routing

This section provides instructions on configuring static, dynamic, and policy-based routing (PBR).

Configuring Static Routing

Static routes are routing information that you manually configure into the router. If the network topology changes, the static route must be updated with a new route. Static routes are private routes, unless they are redistributed by a routing protocol. It is optional to configure static routing on the Cisco 806 router.

To configure static routing, perform the following steps, beginning in global configuration mode.

	Command	Task
Step 1	**ip classless**	Set up a best route for packets destined for networks unknown by the router.
Step 2	**ip route** *network-number mask interface*	Specify the static route for the IP packets.
Step 3	**end**	Exit router configuration mode.

For complete information on the static routing commands, refer to the Cisco IOS Release 12.0 documentation set. For more general information on static routing, see Chapter 1, “Concepts.”

Configuration Example

In the following configuration example, the static route is defined as a default route through the Dialer 0 interface. You would define a default static route through the Dialer interface when using PPPoE. You do not need to enter the commands marked “default.” These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

```
!
ip classless (default)
ip route 0.0.0.0 0.0.0.0 dialer0
ip http server (default)
!
```

Verifying Your Configuration

To verify that you have properly configured static routing, enter the **show ip route** command, and look for static routes, indicated by the “S.” You should see a verification output similar to the following example:

```
router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - 
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS 
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     192.168.89.0/32 is subnetted, 2 subnets
     10.0.0.0/24 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, Ethernet0
S*   0.0.0.0/0 is directly connected, Dialer0
router#
```

Configuring Dynamic Routing

In dynamic routing, the network protocol adjusts the path automatically, based on network traffic or topology. Changes in dynamic routing are shared with other routers in the network.

The IP routing protocol can use Routing Information Protocol (RIP) or Enhanced Interior Gateway Routing Protocol (IGRP) to learn routes dynamically. You can configure either of these routing protocols.

Configuring RIP

To configure RIP routing protocol on the router, perform the following steps, beginning in global configuration mode.

	Command	Task
Step 1	**ip routing**	Enable IP routing.
Step 2	**router rip**	Enter router configuration mode, and enable RIP on the router.
Step 3	**version 2**	Specify use of RIP Version 2.
Step 4	**network** *network-number*	Specify the network number for each directly connected network.
Step 5	**no auto-summary**	Disable automatic summarization of subnet routes into network-level routes. This allows subprefix routing information to transmit across classful network boundries.
Step 6	**end**	Exit router configuration mode.

For complete information on the dynamic routing commands, refer to the Cisco IOS Release 12.0 documentation set. For more general information on RIP, see Chapter 1, “Concepts.”

Configuration Example

The following configuration shows RIP Version 2 enabled in IP network 10.10.10.0.

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

```
!
    router rip
 version 2
 network 10.10.10.0
 no auto-summary
!
```

Verifying Your Configuration

To verify that you have properly configured RIP, enter the **show ip route** command, and look for RIP routes, indicated by the “R.” You should see a verification output similar to the following example:

```
router#show ip route
Codes:C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
    inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, Ethernet0/0
R    3.0.0.0/8 [120/1] via 10.10.10.1, 00:00:02, Ethernet0/0
router#
```

Configuring IP Enhanced IGRP

To configure IP Enhanced IGRP, perform the following steps, beginning in global configuration mode.

	Command	Task
Step 1	**ip routing**	Enable IP routing.
Step 2	**router eigrp** *autonomous-system*	Enter router configuration mode, and enable Enhanced IGRP on the router. The autonomous-system number identifies the route to other Enhanced IGRP routers and is used to tag the Enhanced IGRP information.
Step 3	**network** *network-number*	Specify the network number for each directly connected network.
Step 4	**end**	Exit router configuration mode.

For complete information on the IP Enhanced IGRP commands, refer to the Cisco IOS Release 12.0 documentation set. For more general information on Enhanced IGRP concepts, see Chapter 1, “Concepts.”

Configuration Example

The following configuration shows Enhanced IGRP routing protocol enabled in IP network 10.10.10.0. The Enhanced IGRP autonomous system number is assigned as 100.

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

```
!
router eigrp 100
 network 10.10.10.0
!
```

Verifying Your Configuration

To verify that you have properly configured IP Enhanced IGRP, enter the **show ip route** command, and look for Enhanced IGRP routes, indicated by “D.” You should see a verification output similar to the following example:

```
router#show ip route
Codes:C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

        210.0.0.0/24 is subnetted, 1 subnets
C   10.10.10.0 is directly connected, Ethernet0/0
D    3.0.0.0/8 [90/409600] via 10.10.10.1, 00:00:02, Ethernet0/0
router#
```

Configuring PBR

To configure PBR, you must complete the following tasks:

- Create a route map that specifies the match criteria and the resulting action if all the match clauses are met. Then you must enable PBR for that route map on a particular interface.
- Enable fast-switched PBR by invoking the **ip route-cache policy** command on the appropriate interface.
- Enable local PBR if you want to policy route packets originating from the Cisco 806 router, by specifying a route map in global configuration mode.

For instructions on configuring PBR, refer to the *Cisco IOS Release 12.0 Quality of Service Solutions Configuration Guide.*

Configuring PPPoE Support

Configuring PPPoE support requires the creation of a VPDN, and changes to the Ethernet interfaces and the Dialer interface. To configure Point-to-Point Protocol over Ethernet (PPPoE) support, perform the following steps, beginning in global configuration mode. This procedure includes steps for configuring CHAP authentication. To configure PAP authentication, perform the steps in the following procedure to configure a VPDN and to configure the Ethernet 0 and the Ethernet 1 interface, but perform the steps in "Configuring PAP Authentication" to configure the Dialer interface.

	Command	Task
Step 1	**vpdn enable**	Configure the virtual private dial-up network.
Step 2	**vpdn-group** *tag*	Configure the VPDN group.
Step 3	**request-dialin**	Specify the dialing mode.
Step 4	**protocol pppoe**	Specify the PPPoE protocol for the VPDN group.
Step 5	**interface ethernet 0**	Configure the Ethernet 0 interface for PPPoe support.
Step 6	**ip address** *ip-address subnet-mask*	Set the IP address and subnet mask for the Ethernet 0 interface.
Step 7	**ip tcp adjust-mss 1452**	Specify the maximum segment size for TCP SYN packets.
Step 8	**interface ethernet 1**	Configure the Ethernet 1 interface for PPPoE support.
Step 9	**no ip address**	Disable IP addressing for the Ethernet 1 interface.
Step 10	**pppoe enable**	Enable the PPPoE protocol for the Ethernet 1 interface.
Step 11	**pppoe-client dial-pool-number** *number*	Configure a PPPoE client dial pool.
Step 12	**exit**	Exit Ethernet 1 interface configuration.
Step 13	**interface dialer** *number*	Configure the Dialer interface.

	Command	Task
Step 14	**ip address** { **negotiated** | *ip-address subnet-mask* }	Indicate that the IP address is to be negotiated, or specify an IP address and subnet mask for the Dialer interface.
Step 15	**ip mtu 1492**	Set the size of the maximum IP transmission unit (MTU).
Step 16	**encapsulation ppp**	Specify the encapsulation type.
Step 17	**dialer pool** *pool-number*	Associate the dialer pool configured for the Ethernet 1 interface with the Dialer interface.
Step 18	**dialer-group 1**	Assign the Dialer interface to a dialer list.
Step 19	**ppp authentication chap**	Set the PPP authentication method. In this step, CHAP is specified. Alternatively, you can specify PAP.
Step 20	**end**	Exit router configuration.

Configuring PAP Authentication

If you need to use PAP authentication instead of CHAP, configure the VPDN and the Ethernet interfaces as shown in the previous procedure, but configure the Dialer interface by performing the following steps, beginning in global configuration mode.

	Command	Task
Step 1	**interface dialer** *number*	Configure the Dialer interface.
Step 2	**ip address** { **negotiated** | *ip-address subnet-mask* }	Indicate that the IP address is to be negotiated, or specify an IP address and subnet mask for the Dialer interface.
Step 3	**ip mtu 1492**	Set the size of the maximum IP transmission unit (MTU).
Step 4	**encapsulation ppp**	Specify the encapsulation type.
Step 5	**dialer pool** *pool-number*	Associate the dialer pool configured for the Ethernet 1 interface with the Dialer interface.
Step 6	**dialer-group 1**	Assign the Dialer interface to a dialer list.

	Command	Task
Step 7	**ppp authentication pap callin**	Set the PPP authentication method to PAP, and indicate that the remote system is to be authenticated on incoming calls only.
Step 8	**ppp pap sent-username** *username* **password** *password*	Supply the PAP username and password.
Step 9	**end**	Exit router configuration mode.

Configuration Examples

The following example shows the VPDN configuration, and the Ethernet 0, Ethernet 1, and Dialer 0 interface configurations for PPPoE support. Use the **show running-config** command to view your configuration.

```
vpdn enable
vpdn-group 1
 request-dialin
  protocol pppoe
!

interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
 ip tcp adjust-mss 1452 (required for router to reach all websites)
!
interface Ethernet1
 no ip address
 ip tcp adjust-mss 1452
 pppoe enable
 pppoe-client dial-pool-number 1
!
interface Dialer0
 ip address negotiated
 encapsulation ppp
 dialer pool 1
 dialer group 1
 ppp authentication chap
!
!
```

The following example shows the Dialer configuration when the authentication type is PAP. The VPDN and Ethernet configurations would be the same as in the previous example.

```
!
interface Dialer0
 ip address negotiated
 encapsulation ppp
 dialer pool 1
 dialer group 1
 ppp authentication pap callin
 ppp pap sent-username sohodyne password 70703204E42081B
!
```

Verifying Your Configuration

To verify that you have properly configured PPPoE, enter the **show ip interface dialer** command. The verification output should be similar to the following sample. Not all output has been shown.

```
router#show ip interface dialer 0
Dialer1 is up, line protocol is up
  Internet address is 192.168.89.109/32
  Broadcast address is 255.255.255.255
  Address determined by IPCP
  MTU is 1492 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled.....
```

Configuring Network Address Translation

This section describes how to configure addressing using Network Address Translation (NAT). You can configure NAT for static or dynamic address translations. It contains the following sections:

- Configuring NAT
- Configuring NAT with IPCP

Configuring NAT

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

	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*	Enable dynamic translation of addresses permitted by access list to one of the addresses specified in the pool.
Step 4	**ip nat inside source static** *local-ip global-ip number* **extendable**	Enable static translation of a specified inside local address to a globally unique IP address. This command is optional.
Step 5	**interface ethernet 0**	Enter configuration mode for the Ethernet 0 interface.
Step 6	**ip nat inside**	Establish the Ethernet 0 interface as the inside interface.
Step 7	**exit**	Exit configuration mode for the Ethernet 0 interface.
Step 8	**interface ethernet 1**	Enter configuration mode for the Ethernet 1 interface.
Step 9	**ip nat outside**	Establish the Ethernet 1 interface as the outside interface.
Step 10	**end**	Exit configuration mode for the Ethernet 1 interface and for the router.

For complete information on the NAT commands, refer to the Cisco IOS Release 12.0 documentation set. For more general information on NAT concepts, see Chapter 1, “Concepts.”

Configuration Example

The following configuration example shows NAT configured for the Ethernet 0 and Ethernet 1 interfaces.

The Ethernet 0 interface has an IP address of 192.168.1.1 and a subnet mask of 255.255.255.0. NAT is configured as *inside*, which means that the interface is connected to the inside network that is subject to NAT translation.

The Ethernet 1 interface has an IP address of 192.168.2.1 and a subnet mask of 255.255.255.0. NAT is configured as *outside*, which means that the interface is connected to an outside network, such as the Internet.

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

```
!
interface Ethernet0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast (default)
ip nat inside
!
interface Ethernet1
ip address 192.168.2.1 255.255.255.0
no ip directed-broadcast (default)
ip nat outside
!
ip route 0.0.0.0 0.0.0.0 Ethernet1
!
ip nat pool homenet 192.168.2.1 192.168.2.1 netmask 255.255.255.0
ip nat inside source list 101 pool homenet overload
access-list 101 permit ip 192.168.1.0 0.0.0.255 any
ip classless (default)
!
```

Verifying Your Configuration

To verify that you have properly configured NAT, enter the **show ip nat translation** command. You should see a verification output similar to the following example:

```
router#show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
tcp 192.168.1.1:2267   10.10.10.2:2267    63.148.48.18:80    192.168.2.1:80
utcp 192.168.1.1:2262  10.10.10.2:2262    207.69.188.186:53  192.168.2.1:53
```

```
udp 192.175.89.109:2266 10.10.10.2:2266   207.69.188.186:53  192.168.2.1:53
router#
```

Configuring NAT with IPCP

This section explains how to configure NAT overload and PPP/Internet Protocol Control Protocol (IPCP). With NAT overload configured, you can use one registered IP address for the interface, and you can use it to access the Internet from all the devices in the network.

With PPP/IPCP, the Cisco 806 router automatically negotiates a globally unique (registered or public) IP address for the interface from the ISP route.

To configure NAT overload and IPCP, perform the following steps, beginning in global configuration mode.

	Command	Task
Step 1	**access-list** *access-list-number* **permit** *source* [*source-wildcard*]	Define a standard access list that permits nonregistered IP addresses of hosts.
Step 2	**ip nat inside source list** *access-list-number* **interface dialer 0 overload**	Set up translation of addresses identified by the access list defined in Step 1.
Step 3	**interface ethernet 0**	Enter configuration mode for the Ethernet 0 interface.
Step 4	**ip nat inside**	Establish the Ethernet 0 interface as the inside interface for NAT.
Step 5	**no shutdown**	Enable the Ethernet 0 interface and the configuration changes you just made to it.
Step 6	**exit**	Exit configuration mode for the Ethernet 0 interface.
Step 7	**interface dialer 0**	Enter configuration mode for the Dialer 0 interface.
Step 8	**ip address** *ip-address subnet-mask*	Assign an IP address and subnet mask to the Dialer 0 interface.

	Command	Task
Step 9	**ip nat outside**	Establish the Dialer 0 interface as the outside interface for NAT.
Step 10	**end**	Exit router configuration mode.

For complete information on these commands, refer to the Cisco IOS Release 12.0 documentation set. For more general information on NAT with IPCP concepts, see Chapter 1, "Concepts."

Configuration Example

This configuration example shows the commands relevant to NAT with IPCP configurations. The access list configuration in this example will allow TCP applications such as FTP, Telnet, and HTTP, while blocking raw IP packets. The access list is applied to the Dialer 0 interface.

```
! ACL For Nat
access-list 101 permit ip 192.168.1.0 0.255.255.255 any
ip nat inside source list 101 interface Dialer0 overload
!
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 no shutdown
!
!
interface Ethernet1
 no ip address
 pppoe enable
 pppoe-client dial-pool-number 1
!
!
interface Dialer0
 ip address 140.10.10.5 255.255.255.0
 ip nat outside
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 ppp authentication chap
!
```

Verifying Your Configuration

To verify that you have properly configured NAT, enter the **show ip nat translation** command. You should see a verification output similar to the following example:

```
router#show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
tcp 192.168.1.1:2267   10.10.10.2:2267    63.148.48.18:80    192.168.2.1:80
utcp 192.168.1.1:2262  10.10.10.2:2262    207.69.188.186:53  192.168.2.1:53
udp 192.175.89.109:2266 10.10.10.2:2266   207.69.188.186:53  192.168.2.1:53
router#
```

Configuring Dynamic Host Configuration Protocol

This section explains how to configure the Cisco 806 router for Dynamic Host Configuration Protocol (DHCP) support. It includes the following topics:

- Configuring the DHCP Server and Relay
- Configuring a DHCP Client

Configuring the DHCP Server and Relay

This section explains how to configure the Cisco 806 router as a DHCP server.

With DHCP, LAN devices on an IP network (DHCP clients) can request IP addresses from the DHCP server. The DHCP server allocates IP addresses from a central pool as needed. A DHCP server can be a workstation, a PC, or a Cisco router.

Configuring the DHCP Server

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

	Command	Task
Step 1	**ip dhcp pool** *name*	Enter DHCP configuration mode, and create a pool of IP addresses that can be assigned to DHCP clients.
Step 2	**network** *ip-address subnet-mask*	Specify the network number and mask of the DHCP address pool.
Step 3	**domain-name** *domain name*	Configure the domain name.
Step 4	**dns-server** *ip-address*	Configure the DNS server.
Step 5	**netbios-name-server** *ip-address*	Configure the netbios name server.
Step 6	**default-router** *ip-address*	Designate a default router.
Step 7	**lease** { *days* | **infinite** }	Specify the duration of the lease by specifying the number of days the lease is to extend, or by indicating that the lease is not to expire.
Step 8	**exit**	Exit DHCP configuration mode.

For more information on the features not used in this configuration, refer to the *Cisco IOS DHCP Server* feature module. For more general information on DHCP servers, see Chapter 1, “Concepts.”

Configuration Example

The following example shows commands relevant to a DHCP server configuration. This DHCP server leases its addresses for 100 days.

```
!
ip dhcp pool CLIENT
   network 10.10.10.0 255.255.255.0
   domain-name cisco.com
   default-router 10.10.10.20
   netbios-name-server 10.10.10.40
   dns-server 10.10.10.80
   lease 100
!
```

Verifying Your Configuration

To verify that the server is assigning IP addresses to attached devices, use the s**how ip dhcp binding** command on the DHCP server. You should see a verification output similar to the following example:

```
router#show ip dhcp binding
IP address       Hardware address       Lease expiration        Type
10.10.10.2      0100.80c7.ecd6.70      Sep 02 2001 07:36 PM Automatic
router#
```

Configuring the DHCP Relay

This section describes how to configure the router to forward User Datagram Protocol (UDP) broadcasts, including IP address requests, from DHCP clients. With the DHCP relay feature configured on the Cisco 806 router, the router can relay IP address requests from the LAN interface to the DHCP server.

To configure the DHCP relay, perform the following steps, beginning in global configuration mode.

	Command	Task
Step 1	**interface Ethernet 0**	Enter configuration mode for the Ethernet 0 interface.
Step 2	**ip helper-address** *address*	Forward default UDP broadcasts, including IP configuration requests, to the DHCP server.
Step 3	**no shutdown**	Enable the Ethernet interface and the configuration changes.
Step 4	**exit**	Exit configuration mode for the Ethernet interface.

For complete information on the DHCP relay commands, refer to the Cisco IOS Release 12.0 documentation set. For more general information on DHCP relays, see Chapter 1, “Concepts.”

Configuration Example

The following configuration contains commands relevant to the DHCP relay only.

```
!
interface Ethernet0
ip address 192.168.100.1 255.255.255.0
ip helper-address 200.200.200.1
!
```

Configuring a DHCP Client

If you do not configure PPPoE on the Cisco 806, you may wish to configure a DHCP client for the Ethernet 1 interface. Perform the following steps to configure the router for DHCP client support, starting in global configuration mode.

	Command	Task
Step 1	**interface ethernet 1**	Enter Ethernet 1 interface configuration.
Step 2	**ip address dhcp**	Specify that the Ethernet 1 interface is to receive its IP address from a DHCP server.
Step 3	**end**	Exit router configuration mode.

Configuration Example

The following configuration example shows the commands relevant to the Ethernet 1 interface. These command appear in the configuration file generated when you use the **show running-config** command.

```
!
interface Ethernet1
 ip address dhcp
!
```

Verifying Your Configuration

If the Cisco 806 router is a DHCP client, you can use the **show dhcp lease** command to determine the IP address the router is using, the subnet mask, the lease time, and other useful information.

You should see verification output similar to the following:

```
router# show dhcp lease
```

```
Temp IP addr: 188.188.1.40  for peer on Interface: Ethernet1

Temp sub net mask: 0.0.0.0
   DHCP Lease server: 4.0.0.32, state: 3 Bound

   DHCP transaction id: 2431

   Lease: 3600 secs,  Renewal: 1800 secs,  Rebind: 3150 secs

Temp default-gateway addr: 188.188.1.1
   Next timer fires after: 00:58:01

   Retry count: 0   Client-ID: 0010.7b43.aa01
```

Configuring IP Multicasting

Configure multicast routing by completing the following tasks, starting in global configuration mode.

	Command	Task
Step 1	**ip multicast-routing**	Enable IP multicast forwarding.
Step 2	**ip pim rp-address** *address*	Configure the Protocol Independent Multicasting (PIM) Rendezvous Point (RP) address.
Step 3	**interface ethernet 0**	Enter Ethernet 0 interface configuration mode.
Step 4	**ip address** *ip-address subnet-mask*	Configure an IP address and subnet mask for the Ethernet 0 interface.
Step 5	**ip pim** { **sparse** | **dense** }**-mode**	Configure the Ethernet 0 interface for PIM sparse mode or PIM dense mode.
Step 6	**interface dialer** *number*	Enter Dialer interface configuration mode.
Step 7	**ip address** { *ip-address subnet-mask* | **negotiated** }	Specify an IP address and subnet mask for the Dialer interface, or indicate that the IP address is to be negotiated.

	Command	Task
Step 8	**ip pim** { **sparse** | **dense** }**-mode**	Configure the Dialer interface for PIM sparse mode or PIM dense mode.
Step 9	**end**	Exit router configuration mode.

Configuration Example

The following example shows the relevant multicast-routing commands. The Ethernet 0 and the Dialer 0 interfaces have been configured for PIM sparse mode, and the PIM RP address has been defined as 192.168.20.3.

```
!
hostname R1
!
ip subnet-zero
ip multicast-routing
ip pim rp-address 192.168.20.3
!
!
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
 ip pim sparse-mode
!
!
interface Dialer0
 ip address 140.10.10.5 255.255.255.0
 ip pim sparse-mode
 ip route-cache
!
```

Verifying Your Configuration

You can verify your configuration of multicasting by using the **show ip igmp interface ethernet 0** command. You should see verification output similar to the following:

```
router#show ip igmp interface ethernet 0
Ethernet0 is up, line protocol is up
  Internet address is 192.168.1.1/24
  IGMP is enabled on interface
  Current IGMP host version is 2
  Current IGMP router version is 2
  IGMP query interval is 60 seconds
  IGMP querier timeout is 120 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1000 ms
  Inbound IGMP access group is not set
  IGMP activity:1 joins, 0 leaves
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  Multicast designated router (DR) is 12.0.0.1 (this system)
  IGMP querying router is 12.0.0.1 (this system)
  Multicast groups joined (number of users):
      224.0.1.40(1)
```

Configuring an Extended Access List

To include one or more extended access lists in your router configuration, complete the following steps, beginning in global configuration mode.

Note Extended access lists can be given tags consisting of numbers from 100 through 199, or they can be given alphanumeric tags. Alphanumeric tags must begin with a letter and must not contain any spaces.

	Command	Task
Step 1	**access-list** *tag* **permit tcp any ip** *ip address-mask* **established**	Permit any host on the network to access any Internet server.
Step 2	**access-list** *tag* **deny ip** *ip adddress-mask* **any**	Deny any Internet host from spoofing any host on the network.
Step 3	**access-list** *tag* **permit tcp host** *ip address-mask*	Permit the Internet DNS server to send TCP replies to any host on the network.
Step 4	**access-list** *tag* **permit udp host** *ip address-mask*	Permit the Internet DNS server to send UDP replies to any host on the network.
Step 5	**access-list** *tag* **permit tcp any host** *ip address*	Permit the Simple Mail Transfer Protocol (SMTP) mail server to access any Internet server.
Step 6	**access-list** *tag* **permit tcp any host** *ip address*	Permit the web server to access any Internet server.
Step 7	**access-list** *tag* **permit icmp any any** *icmp-message-type*	Permit ICMP messages of the specified type to be sent or received.
Step 8	**access-list** *tag* **deny tcp any** *ip address-mask*	Restrict any Internet host from making a Telnet connection to any host on the network.
Step 9	**interface dialer** *number*	Enter configuration mode for the Dialer interface.
Step 10	**ip access-group** *tag* **in**	Activate the access list of the specified tag.
Step 11	**exit**	Exit configuration mode for the Dialer interface.

For more complete information on the extended access list commands, refer to the Cisco IOS Release 12.0 documentation set. For information on TCP and UDP port assignments, see Appendix C, "Common Port Assignments."

Configuration Example

This configuration shows an access list being applied to IP address 198.92.32.130.

```
!
access-list 101 permit tcp any host 198.92.32.130 0.0.0.255
!
```

Verifying Your Configuration

Use the **show access-lists** command to verify access list configuration. The following example shows sample output for all access lists with the tag 101:

```
router> show access-lists 105

Extended IP access list 105
    permit icmp any any echo-reply
    permit icmp any any time-exceeded
    permit icmp any any packet-too-big
    permit icmp any any traceroute
    permit icmp any any unreachable
    deny ip host 255.255.255.255 any
    deny ip 192.168.1.0 0.0.0.255 any
```

Configuring Network Time Protocol Support

The Network Time Protocol (NTP) is a protocol designed to time-synchronize a network of machines. NTP runs over UDP, which runs over IP. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to within a millisecond of one another.

To identify a Network Time Protocol (NTP) server on the network and configure the Cisco 806 router as an NTP client, enter the following command in global configuration mode:

ntp server *ip-address*

where *ip-address* is the address of an NTP server on the network.

To configure the Cisco 806 router function as an NTP server, enter the following command in global configuration mode:

ntp master *stratum-number*

where *stratum-number* indicates the number of hops between the Cisco 806 router and an authorotative time source.

Configuring IP Security and Generic Routing Encapsulation Tunneling

IP Security (IPSec) provides secure tunnels between two peers, such as two routers. You define which packets are to be considered sensitive and thus should be sent through these secure tunnels. You also define the parameters which should be used to protect these sensitive packets, by specifying characteristics of these tunnels. Then, when the IPSec peer sees a sensitive packet, it sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer.

The configuration of IPSec and GRE tunneling are presented together in this section. To configure IPSec using a GRE tunnel, perform the following steps, beginning in global configuration mode.

	Command	Task
Step 1	**crypto isakmp policy 10**	Define an Internet Key Exchange (IKE) policy, and assign the policy a priority. This command places the router in IKE policy configuration mode.
Step 2	**hash md5**	Specify the md5 hash algorithm for the policy.
Step 3	**authentication pre-share**	Specify pre-share key as the authentication method.
Step 4	**exit**	Exit IKE policy configuration mode.
Step 5	**access-list 101 permit gre host** *starting-ip-address* **host** *ending-ip-address*	Create an access list that permits the GRE protocol, and that specifies the IP addresses of the starting and ending points of the GRE tunnel.

	Command	Task
Step 6	**crypto isakmp key** *name* **address** *ip-address*	Configure a pre-shared key and static IP address for each VPN client.
Step 7	**crypto ipsec transform-set** *name* **esp-des esp-md5-hmac**	Define a combination of security associations to occur during IPSec negotiations.
Step 8	**crypto map** *name* **local-address ethernet 1**	Enter crypto map configuration mode, and specify and name an identifying interface to be used by the crypto map for IPSec traffic.
Step 9	**crypto map** *name seq-num* **ipsec-isakmp**	Create a crypto map entry in IPSec ISAKMP mode, and enter crypto map configuration mode.
Step 10	**set peer** *ip-address*	Identify the remote IPSec peer.
Step 11	**set transform-set** *name*	Specify the transform set to be used.
Step 12	**match address** *access-list-id*	Specify an extended access list for the crypto map entry.
Step 13	**exit**	Exit crypto map configuration mode.
Step 14	**interface ethernet 1**	Configure the Ethernet 1 interface.
Step 15	**ip address** *ip-address subnet-mask*	Set the IP address and subnet mask for the Ethernet 1 interface.
Step 16	**crypto map** *name*	Associate the crypto map with the Ethernet 1 interface.
Step 17	**exit**	Exit Ethernet 1 interface configuration mode.
Step 18	**interface tunnel 0**	Configure the Tunnel 0 interface.
Step 19	**ip address** *ip-address subnet-mask*	Set the IP address and subnet mask for the Tunnel 0 interface.
Step 20	**tunnel source ethernet 1**	Specify the Ethernet 1 interface as the tunnel source.
Step 21	**tunnel destination** *default-gwy-ip-address*	Specify the default gateway as the tunnel destination.
Step 22	**crypto map** *name*	Associate the crypto map to the Tunnel 0 interface.
Step 23	**end**	Exit router configuration mode.

For more information on configuring IPSec and GRE tunneling, refer to the *Cisco IOS Security Configuration Guide*.

Configuration Example

The following configuration example shows the commands relevant to IPSec and and GRE tunneling. Note that the crypto map named mymap is associated with the Tunnel 0 interface and with the Ethernet 1 interface, and that the tunnel destination address of 140.10.10.6 matches the end point address in the access list.

```
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 140.10.10.6
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap local-address Ethernet1
crypto map mymap 10 ipsec-isakmp
 set peer 140.10.10.6
 set transform-set myset
 match address 101
!
interface Tunnel0
 ip address 11.0.0.1 255.0.0.0
 tunnel source Ethernet1
 tunnel destination 140.10.10.6
 crypto map mymap
!
!
interface Ethernet1
 ip address 140.10.10.5 255.255.255.0
 crypto map mymap
!
access-list 101 permit gre host 140.10.10.5 host 140.10.10.6
!
```

Configuring Other Security Features

This section provides information about the security features available on the Cisco 806 router.

Configuring a RADIUS Client

Remote Authentication Dial-In User Service (RADIUS) enables you to secure your network agains unauthorized access. A RADIUS server must be configured in the service provider or corporate network in order for the Cisco 806 to use RADIUS client features.

To configure RADIUS on your Cisco 806 router, you must perform the following tasks:

- Use the **aaa new-model** global configuration command to enable Authentication, Authorization, and Accounting (AAA). AAA must be configured if you plan to use RADIUS.
- Use the **aaa authentication** global configuration command to define method lists for RADIUS authentication.
- Use line and interface commands to enable the defined method lists to be used.

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

Configuring TACACS+

To configure your router to support TACACS+, you must perform the following tasks:

- Use the **aaa new-model** global configuration command to enable AAA. AAA must be configured if you plan to use TACACS+.
- Use the **tacacs-server host** command to specify the IP address of one or more TACACS+ daemons. Use the tacacs-server key command to specify an encryption key that will be used to encrypt all exchanges between the network access server and the TACACS+ daemon. This same key must also be configured on the TACACS+ daemon.

- Use the **aaa authentication** global configuration command to define the method lists that use TACACS+ for authentication.
- Use line and interface commands to apply the defined method lists to various interfaces.

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

Configuring Service Assurance Agent Support

The Cisco Service Assurance Agent (SA Agent) is an application-aware synthetic operation agent that monitors network performance by measuring key metrics such as response time, availability, jitter (interpacket delay variance), connect time, throughput, and packet loss. These metrics can be used for troubleshooting, for analysis for prevention of problems, and for designing future network topologies.

For instructions on configuring SA Agent support, refer to the Cisco IOS Release 12.0 documentation set.

CHAPTER 4

Troubleshooting

Use the information in this chapter to help isolate problems you might encounter with the Cisco 806 router or to rule out the router as the source of the problem. This chapter contains the following sections:

- Before Contacting Cisco or Your Reseller
- Troubleshooting Commands
- Software Upgrade Methods
- Recovering a Lost Password

Before troubleshooting a software problem, you must connect a terminal or PC to the router via the light-blue console port. (For information on making this connection, refer to the *Cisco 806 Router Hardware Installation Guide*.) With a connected terminal or PC, you can read status messages from the router and enter commands to troubleshoot a problem.

You can also remotely access the interface (Ethernet, or telephone) by using Telnet. The Telnet option assumes that the interface is up and running.

Before Contacting Cisco or Your Reseller

If you cannot locate the source of a problem, contact your local reseller for advice. Before you call, you should have the following information ready:

- Chassis type and serial number
- Maintenance agreement or warranty information
- Type of software and version number

- Date you received the hardware
- Brief description of the problem
- Brief description of the steps you have taken to isolate the problem

Troubleshooting Commands

This section describes some commonly used troubleshooting commands.

Show Interface Command

Use the **show interface** command to display the status of all physical ports (Ethernet and logical interfaces on the router. To display the status of a single interface, add the name of the interface to the end of the command. The following example shows output for the Dialer0 interface:

```
router#show interface dialer 0
Dialer0 is up (spoofing), line protocol is up (spoofing)
  Hardware is Unknown
  Internet address will be negotiated using IPCP
  MTU 1500 bytes, BW 56 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
  DTR is pulsed for 1 seconds on reset
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 03:12:51
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops:0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/16 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 42 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes
     0 packets output, 0 bytes
router#
```

show flash Command

Use the **show flash** command to display the name of the software image that is in Flash memory. The command output also includes information on Flash memory usage.

```
router#show flash

System flash directory:
File  Length   Name/status
  1   3260404  c806-sy6-mz
[3260468 bytes used, 5128140 available, 8388608 total]
8192K bytes of processor board System flash (Read/Write)

router#
```

Debug Commands

This section describes how to use debug commands with additional keywords to troubleshoot the router.

Before Using Debug Commands

You can use the debug commands to troubleshoot configuration problems that you might be having on your network. Debug commands provide extensive, informative displays to help you interpret any possible problems. All debug commands are entered in privileged EXEC mode, and most debug commands take no arguments. Read the information in Table 4-1 before using debug commands.

⚠ **Caution** Debugging is assigned a high priority in your router CPU process, and it can render your router unusable. For this reason, use debug commands only for troubleshooting specific problems. The best time to use debug commands is during periods of low network traffic so that other activity on the network is not adversely affected.

Table 4-1 Important Information About Debug Commands

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

debug ethernet-interface Command

Use the **debug ethernet-interface** command to troubleshoot the Ethernet interfaces.

Sample **debug ethernet-interface** command output follows:

```
router>debug ethernet-interface
3d04h: %PQUICC_FE-5-LOSTCARR: PQUICC/FE(0/0), Lost carrier.
Transceiver problem?
3d04h: FEC interrupt 32822 (tx=32822,rx=0,er=0)
```

debug ip dhcp server events Command

Use the **debug ip dhcp server events** command for DHCP troubleshooting:

```
router#debug ip dhcp server events
```

```
1d21h: DHCPD: there is no address pool for 1.7.45.35.
```

debug ppp negotiation Command

Use the **debug ppp negotiation** command to monitor PPP negotiation events.

Sample **debug ppp negotiation** command output follows:

```
router# debug ppp negotiation
ppp: sending CONFREQ, type = 4 (CI_QUALITYTYPE), value = C025/3E8
ppp: sending CONFREQ, type = 5 (CI_MAGICNUMBER), value = 3D56CAC
ppp: received config for type = 4 (QUALITYTYPE) acked
ppp: received config for type = 5 (MAGICNUMBER) value = 3D567F8 acked
(ok)
PPP Dialer1: state = ACKSENT fsm_rconfack(C021): rcvd id 5
ppp: config ACK received, type = 4 (CI_QUALITYTYPE), value = C025
ppp: config ACK received, type = 5 (CI_MAGICNUMBER), value = 3D56CAC
ppp: ipcp_reqci: returning CONFACK.
 (ok)
PPP Dialer1: state = ACKSENT fsm_rconfack(8021): rcvd id 4
```

debug ip packet Command

Use the **debug ip packet** command to troubleshoot IP problems.

Sample **debug ip packet** output follows:

```
router>debug ip packet
3d04h: IP: s=192.168.1.1 (local), d=223.255.254.253 (Ethernet0),
len 100, encapsulation failed.!
3d04h: IP: s=192.168.1.1 (local), d=223.255.254.253 (Ethernet0),
len 100, sending
3d04h: IP: s=192.168.2.1 (Ethernet0), d=1.7.45.35 (Ethernet0),
len 100, rcvd 3
3d04h: IP: s=192.168.1.1 (local), d=223.255.254.253 (Ethernet0),
len 100, sending
```

Software Upgrade Methods

These are the methods for upgrading software on the Cisco 806 router:

- Copy the new software image to Flash memory over the LAN or WAN while the existing Cisco IOS software image is operating.
- Copy the new software image to Flash memory over the LAN while the boot image (ROM monitor) is operating.

- Copy the new software image over the console port while in ROM monitor mode.
- While in ROM monitor mode, boot the router from a software image that is loaded on a TFTP server. To use this method, the TFTP server must be on the same LAN as the router.

Recovering a Lost Password

This section describes how to recover a lost enable or enable secret password. The process of recovering a password comprises the following major tasks:

- Changing the Configuration Register
- Resetting the Router
- Resetting the Password and Saving Your Changes (for lost enable secret passwords only)
- Resetting the Configuration Register Value

Note These procedures can be done only when you are connected to the router through the console port. These procedures cannot be performed through a Telnet session.

Note See the "Hot Tips" section on Cisco.com for additional information on replacing enable secret passwords.

Changing the Configuration Register

To change a configuration register, perform the following steps:

Step 1 Connect an ASCII terminal or a PC running a terminal emulation program to the CONSOLE port on the rear panel of the router. Refer to the “Connecting the Router to a PC”section in Chapter 2, “Installation,” in the *Cisco 806 Router Hardware Installation Guide*.

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

Step 3 At the privileged EXEC prompt (*router_name* #), enter the **show version** command to display the existing configuration register value. The following example contains partial output from the **show version** command. The configuration register value is shown at the end of the command output.

```
router#show version
Cisco Internetwork Operating System Software
IOS (tm) C806 Software (C806-SY6-M), Experimental Version
12.2(20010417:231612)
.....
Configuration register is 0x2102

router#
```

Step 4 Record the setting of the configuration register. (It is usually 0x2102 or 0x100.)

Step 5 Record the break setting:

- Break enabled—Bit 8 is set to 0.
- Break disabled (default setting)—Bit 8 is set to 1.

Note To enable break, enter the **config-register 0x01** command while in privileged EXEC mode.

Resetting the Router

To reset the router, perform the following steps:

Step 1 If break is enabled, go to Step 2. If break is disabled, unplug the router, wait 5 seconds, and plug it back in again. Within 60 seconds, press the **Break** key. The terminal displays the ROM monitor prompt. Go to Step 3.

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

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

```
rommon 2>
```

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

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

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

```
rommon 2> reset
```

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

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

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

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

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

```
Router>
```

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

```
Router> enable
```

The prompt changes to the privileged EXEC prompt:

```
Router#
```

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

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

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

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

Resetting the Password and Saving Your Changes

To reset your password and save the changes, perform the following steps:

Step 1 Enter the **configure terminal** command to enter configuration mode:

```
Router# configure terminal
```

Step 2 Enter the **enable secret** command to reset the enable secret password in the router:

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

Step 3 Enter **exit** to exit configuration mode:

```
Router(config)# exit
```

Step 4 Save your configuration changes:

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

Resetting the Configuration Register Value

After you have recovered or reconfigured a password, reset the configuration register value:

Step 1 Enter the **configure terminal** command to enter configuration mode:

```
Router# configure terminal
```

Step 2 Enter the **configure register** command and the original configuration register value that you recorded.

```
Router(config)# config-reg value
```

Step 3 Enter **exit** to exit configuration mode:

```
Router(config)# exit
```

Note To return to the configuration in use before you recovered the lost enable password, do not save the configuration changes before you reboot the router.

Step 4 Reboot the router, and enter the recovered password.

Cisco IOS Basic Skills

Understanding how to use Cisco IOS software saves time when you are configuring your router. If you need a refresher, take a few minutes to read this chapter. If you are already familiar with Cisco IOS software, go to Chapter 3, "Feature-by-Feature Router Configurations."

This chapter describes what you need to know before you begin configuring your Cisco 806 router with Cisco IOS software (the software that runs your router).

This chapter contains the following sections:

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

Configuring the Router from a PC

You can configure your router from a connected PC. For information on how to connect the PC, refer to the *Cisco 806 Routers Hardware Installation Guide*.

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

Table 0-1 Terminal Emulation Software

PC Operating System	Software
Windows 95, Windows 98, Windows 2000, Windows Millenium Edition, Windows NT	HyperTerm (included with Windows software), ProComm Plus
Windows 3.1	Terminal (included with Windows software)
Macintosh	ProComm, VersaTerm (supplied separately)

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

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

These settings should match the default settings of your router. To change the router baud, data bits, parity, or stop bits settings, you must reconfigure parameters in the ROM monitor. For more information, see Appendix B, "ROM Monitor." To change the router flow control setting, use the **flowcontrol** line configuration command.

For information on how to enter global configuration mode so that you can configure your router, see “Entering Global Configuration Mode” in this chapter.

Understanding Command Modes

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

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

- User EXEC
- Privileged EXEC
- Global configuration

Table A-2 lists the command modes that are used in this guide, how to access each mode, the prompt you see in that mode, and how to exit to a mode or enter the next mode. Because each mode configures different router elements, you might need to enter and exit modes frequently. You can see a list of available commands for a particular mode by entering a question mark (?) at the prompt. For a description of each command, including syntax, refer to the Cisco IOS Release 12.0 documentation set.

Table 0-2 Command Modes Summary

Mode	Access Method	Prompt	Exit/Entrance Method	About This Mode
User EXEC	Begin a session with your router.	`Router>`	To exit the router session, enter the **logout** command.	Use this mode to • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	Enter the **enable** command from user EXEC mode.	`Router#`	To exit to user EXEC mode, enter the **disable** command. To enter global configuration mode, enter the **configure** command.	Use this mode to • Configure your router operating parameters. • Perform the verification steps shown in this guide. • To prevent unauthorized changes to your router configuration, access to this mode should be protected with a password as described in “Enable Secret and Enable Passwords” later in this chapter.

Table 0-2 Command Modes Summary (continued)

Mode	Access Method	Prompt	Exit/Entrance Method	About This Mode
Global configuration	Enter the **configure** command from privileged EXEC mode.	`Router (config)#`	To exit to privileged EXEC mode, enter the **exit** or **end** command, or press **Ctrl-Z**. To enter interface configuration mode, enter the **interface** command.	Use this mode to configure parameters that apply to your router as a whole. Also, you can access the following modes, which are described in this table: • Interface configuration • Router configuration • Line configuration
Interface configuration	Enter the **interface** command (with a specific interface, such as **interface ethernet 0**) from global configuration mode.	`Router (config-if)#`	To exit to global configuration mode, enter the **exit** command. To exit to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**. To enter subinterface configuration mode, specify a subinterface with the **interface** command.	Use this mode to configure parameters for the router Ethernet and serial interfaces or subinterfaces.

Table 0-2 Command Modes Summary (continued)

Mode	Access Method	Prompt	Exit/Entrance Method	About This Mode
Router configuration	Enter your router command followed by the appropriate keyword, for example **router rip**, from global configuration mode.	`Router (config-router)#`	To exit to global configuration mode, enter the **exit** command. To exit to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.	Use this mode to configure an IP routing protocol.
Line configuration	Specify the **line** command with the desired keyword, for example, **line 0**, from global configuration mode.	`Router (config-line)#`	To exit to global configuration mode, enter the **exit** command. To enter privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.	Use this mode to configure parameters for the terminal line.

Getting Help

You can use the question mark (?) and arrow keys to help you enter commands.

For a list of available commands at a command mode, enter a question mark:

```
router> ?
access-enable   Create a temporary access-list entry
access-profile  Apply user-profile to interface
clear           Reset functions
...
```

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

```
router> s?
* s=show set show slip systat
```

For a list of command variables, enter the command, followed by a space and a question mark:

```
router> show ?
clock       Display the system clock
dialer      Dialer parameters and statistics
exception   exception information
...
```

To redisplay a command you previously entered, press the **Up Arrow** key. You can continue to press the **Up Arrow** key for more commands.

Enable Secret and Enable Passwords

By default, the router ships without password protection. Because many privileged EXEC commands are used to set operating parameters, you should password-protect these commands to prevent unauthorized use.

You can use two commands to do this:

- **enable secret** *password* (a very secure, encrypted password)
- **enable** *password* (a less secure, unencrypted password)

You must enter an **enable secret** password to gain access to privileged EXEC mode commands.

For maximum security, the passwords should be different. If you enter the same password for both during the setup process, your router accepts the passwords, but warns you that they should be different.

An **enable secret** password can contain from 1 to 25 uppercase and lowercase alphanumeric characters. An **enable** password can contain any number of uppercase and lowercase alphanumeric characters. In each case, the first character cannot be a number. Spaces are also valid password characters; for example, *two words* is a valid password. Leading spaces are ignored; trailing spaces are recognized.

Entering Global Configuration Mode

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

To enter global configuration mode:

Step 1 After your router boots up, answer **no** when the following question displays:

```
Would you like to enter the initial configuration dialog [yes]: no
```

Step 2 Enter the **enable** command:

```
router> enable
```

Step 3 If you have configured your router with an enable password, enter it when you are prompted.

The enable password does not show on the screen when you enter it. This example shows how to enter privileged EXEC mode:

```
Password: enable_password
router#
```

Enable mode is indicated by the # in the prompt.

Step 4 Enter the **configure terminal** command to enter global configuration mode, indicated by `(config)#` in the prompt:

```
router# configure terminal
router (config)#
```

You can now make changes to your router configuration.

Using Commands

This section provides some tips about entering Cisco IOS commands at the command-line interface (CLI).

Abbreviating Commands

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

```
router # sh v
```

Undoing Commands

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

Command-Line Error Messages

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

Table 0-3 Common CLI Error Messages

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

Saving Configuration Changes

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

```
router # copy running-config startup-config
Destination filename [startup-config]?
```

Press **Return** to accept the default destination filename startup-config, or enter your desired destination filename and press **Return**.

It might take a minute or two to save the configuration to NVRAM. After the configuration has been saved, the following message appears:

```
Building configuration...
router #
```

Summary

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

- You can use the question mark (**?**) and arrow keys to help you enter commands.
- Each command mode restricts you to a set of commands. If you are having difficulty entering a command, check the prompt, and then enter the question mark (**?**) for a list of available commands. You might be in the wrong command mode or might be using the wrong syntax.
- If you want to disable a feature, enter the keyword **no** before the command; for example, **no ip routing**.
- Save your configuration changes to NVRAM so that they are not lost if there is a system reload or power outage.

Where to Go Next

To configure your router, see Chapter 3, “Feature-by-Feature Router Configurations.”

CHAPTER B

ROM Monitor

This appendix describes the Cisco 806 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 use the ROM monitor to perform certain configuration tasks, such as recovering a lost password or downloading software over the console port. If there is no Cisco IOS software image loaded on the router, the ROM monitor runs the router.

This appendix contains the following sections:

- Entering the ROM Monitor
- ROM Monitor Commands
- Command Descriptions
- Disaster Recovery with TFTP Download
- Configuration Register
- Console Download
- Debug Commands
- Exiting the ROM Monitor

Entering the ROM Monitor

To use the ROM monitor, you must be using a terminal or PC that is connected to the router over the console port. Refer to the installation chapter in the *Cisco 806 Router Hardware Installation Guide* that came with the router to connect the router to a PC or terminal.

Perform these steps to configure the router to boot up in ROM monitor mode the next time it is rebooted.

	Command	Task
Step 1	**enable**	If an enable password is configured, enter the enable command and the enable password to enter privileged EXEC mode.
Step 2	**configure terminal**	Enter global configuration mode.
Step 3	**config-reg 0x0**	Reset the configuration register.
Step 4	**exit**	Exit global configuration mode.
Step 5	**reload**	Reboot the router with the new configuration register value. The router remains in ROM monitor and does not boot the Cisco IOS software. As long as the configuration value is 0x0, you must manually boot the operating system from the console. See the **boot** command in the “Command Descriptions” section in this appendix. After the router reboots, it is in ROM monitor mode. The number in the prompt increments with each new line.

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

ROM Monitor Commands

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

```
rommon 1 > ?
alias               set and display aliases command
boot                boot up an external process
break               set/show/clear the breakpoint
confreg             configuration register utility
cont                continue executing a downloaded image
context             display the context of a loaded image
cookie              display contents of cookie PROM in hex
dev                 list the device table
dir                 list files in file system
dis                 display instruction stream
dnld                serial download a program module
frame               print out a selected stack frame
help                monitor builtin command help
history             monitor command history
meminfo             main memory information
repeat              repeat a monitor command
reset               system reset
set                 display the monitor variables
stack               produce a stack trace
sync                write monitor environment to NVRAM
sysret              print out info from last system return
tftpdnld            tftp image download
unalias             unset an alias
unset               unset a monitor variable
xmodem              x/ymodem image download
```

Commands are case sensitive. You can halt any command by pressing the Break key on a terminal. If you are using a PC, most terminal emulation programs halt a command when you press the Ctrl and the Break keys at the same time. If you are using another type of terminal emulator or terminal emulation software, refer to the documentation for that product for information on how to send a Break command.

Command Descriptions

Table B-1 describes the most commonly used ROM monitor commands.

Table 0-1 Most Commonly Used ROM Monitor Commands

<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td><b>help</b> or <b>?</b></td><td>Displays a summary of all available ROM monitor commands.</td></tr>
<tr><td><b>-?</b></td><td>Displays information about command syntax; for example:
<pre>
rommon 16 > <b>dis -?</b>
usage : dis [addr] [length]
</pre>
The output for this command is slightly different for the <b>xmodem</b> download command:
<pre>
rommon 11 > <b>xmodem -?</b>
xmodem: illegal option -- ?
usage: xmodem [-cyrxu] <destination filename>
-c CRC-16
-y ymodem-batch protocol
-r copy image to dram for launch
-x do not launch on download completion
-u upgrade ROMMON, System will reboot after upgrade
</pre></td></tr>
<tr><td><b>reset</b> or <b>i</b></td><td>Resets and initializes the router, similar to a power up.</td></tr>
<tr><td><b>dev</b></td><td>Lists boot device identifications on the router; for example:
<pre>
rommon 10> <b>dev</b>
Devices in device table:
        id name
    flash: flash
</pre></td></tr>
<tr><td><b>dir</b> <i>device</i><b>:</b></td><td>Lists the files on the named device; flash, for example:
<pre>
rommon 4 > dir flash:
      File size   Checksum   File name
2835276 bytes (0x2b434c)   0x2073   c806-oy6-mz
</pre></td></tr>
<tr><td>boot commands</td><td>For more information about the ROM monitor boot commands, refer to the <i>Cisco IOS Configuration Guide</i> and the <i>Cisco IOS Command Reference.</i></td></tr>
<tr><td><b>b</b></td><td>Boots the first image in Flash memory.</td></tr>
<tr><td><b>b flash:</b> [<i>filename</i>]</td><td>Attempts to boot the image directly from the first partition of Flash memory. If you do not enter a filename, this command will boot this first image in Flash.</td></tr>
</table>

Disaster Recovery with TFTP Download

The standard way to load new software on your router is using the **copy tftp flash** privileged EXEC command from the Cisco IOS software command-line interface (CLI). However, if the router is unable to boot the Cisco IOS software, you can load new software while in ROM monitor mode.

This section describes how to load a Cisco IOS software image from a remote TFTP server to the router Flash memory. Use the **tftpdnld** command only for disaster recovery because it erases all existing data in Flash memory before downloading a new software image to the router.

TFTP Download Command Variables

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

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

Required Variables

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

Variable	Command
IP address of the router.	**IP_ADDRESS=** *ip_address*
Subnet mask of the router.	**IP_SUBNET_MASK=** *ip_address*
IP address of the default gateway of the router.	**DEFAULT_GATEWAY=** *ip_address*

Variable	Command
IP address of the TFTP server from which the software will be downloaded.	**TFTP_SERVER=** *ip_address*
The name of the file that will be downloaded to the router.	**TFTP_FILE=** *filename*

Optional Variables

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

Variable	Command
Configures how the router displays file download progress. **0**—No progress is displayed. **1**—Exclamation points (!!!) are displayed to indicate file download progress. This is the default setting. **2**—Detailed progress is displayed during the file download process; for example: • Initializing interface. • Interface link state up. • ARPing for 1.4.0.1 • ARP reply for 1.4.0.1 received. MAC address 00:00:0c:07:ac:01	**TFTP_VERBOSE=** *setting*
Number of times the router attempts ARP and TFTP download. The default is 7.	**TFTP_RETRY_COUNT=** *retry_times*

Variable	Command
Amount of time, in seconds, before the download process times out. The default is 2,400 seconds (40 minutes).	**TFTP_TIMEOUT=** *time*
Whether or not the router performs a checksum test on the downloaded image: **1**—Checksum test is performed. **0**—No checksum test is performed.	**TFTP_CHECKSUM=***setting*

Using the TFTP Download Command

The steps described in this section should be performed while in ROM monitor mode.

Step 1 Use the appropriate commands to enter all the required variables and any optional variables described earlier in this section.

Step 2 Enter the **tftpdnld** command as follows:

```
rommon 1 > tftpdnld -r
```

Note The **-r** variable is optional. Entering this variable downloads and boots the new software but does not save the software to Flash memory. You can then use the image that is in Flash memory the next time you enter the **reload** command.

You will see output similar to the following:

```
IP_ADDRESS: 1.3.6.7
      IP_SUBNET_MASK: 255.255.0.0
     DEFAULT_GATEWAY: 1.3.0.1
         TFTP_SERVER: 223.255.254.254
           TFTP_FILE: c806-sy-mz
Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash will be lost!
Do you wish to continue? y/n:  [n]:
```

Step 3 If you are sure that you want to continue, enter **y** in response to the question in the output:

```
Do you wish to continue? y/n:  [n]:y
```

The router begins to download the new file.

Enter **Ctrl-C** or **Break** to stop the transfer before the Flash memory is erased.

Configuration Register

The virtual configuration register is in nonvolatile RAM (NVRAM) and has the same functionality as other Cisco routers. You can view or modify the virtual configuration register from either the ROM monitor or the operating system software. Within ROM monitor, you can change the configuration register by entering the register value in hexadecimal format, or by allowing the ROM monitor to prompt you for the setting of each bit.

Changing the Configuration Register Manually

To change the virtual configuration register from the ROM monitor manually, enter the command **confreg** followed by the new value of the register in hexadecimal, as shown in the following example:

```
rommon 1 > confreg 0x2101


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

The value is always interpreted as hexadecimal. The new virtual configuration register value is written into NVRAM but does not take effect until you reset or reboot the router.

Changing the Configuration Register Using Prompts

Entering **confreg** without an argument displays the contents of the virtual configuration register and a prompt to alter the contents by describing the meaning of each bit.

In either case, the new virtual configuration register value is written into NVRAM but does not take effect until you reset or reboot the router.

The following display shows an example of entering the **confreg** command:

```
rommon 7> confreg

     Configuration Summary
enabled are:
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:  y
enable  “diagnostic mode”? y/n  [n]:  y
enable  “use net in IP bcast address”? y/n  [n]:
enable  “load rom after netboot fails”? y/n  [n]:
enable  “use all zero broadcast”? y/n  [n]:
enable  “break/abort has effect”? y/n  [n]:
enable  “ignore system config info”? y/n  [n]:
change console baud rate? y/n  [n]:  y
enter rate: 0 = 9600, 1 = 4800, 2 = 1200, 3 = 2400  [0]:  0
change the boot characteristics? y/n  [n]:  y
enter to boot:
 0 = ROM Monitor
 1 = the boot helper image
 2-15 = boot system
    [0]:  0

Configuration Summary
enabled are:
diagnostic mode
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:


You must reset or power cycle for new config to take effect
```

Console Download

You can use console download, a ROM monitor function, to download over the router console port either a software image or a configuration file. After download, the file is either saved to the mini-Flash memory module or to main memory for execution (image files only).

Use console download when you do not have access to a Trivial File Transfer Protocol (TFTP) server.

Note If you want to download a software image or a configuration file to the router over the console port, you must use the **ROM monitor** command.

Note If you are using a PC to download a Cisco IOS image over the router console port at 115,200 bps, ensure that the PC serial port is using a 16550 universal asynchronous transmitter/receiver (UART). If the PC serial port is not using a 16550 UART, we recommend using a speed of 38,400 or less when downloading a Cisco IOS image over the console port.

Command Description

The following are the syntax and descriptions for the **xmodem** console download command:

`xmodem [-cyrx]` *`destination_file_name`*

where

c	Optional. Performs the download using 16-bit cyclic redundancy check (CRC-16) error checking to validate packets. Default is 8-bit CRC.

y Optional. Sets the router to perform the download using Ymodem protocol. Default is Xmodem protocol. The protocols differ as follows:

- Xmodem supports a 128-block transfer size. Ymodem supports a 1024-block transfer size.
- Ymodem uses (CRC)-16 error checking to validate each packet. Depending on the device that the software is being downloaded from, this function might not be supported by Xmodem.

r Optional. Image is loaded into DRAM for execution. Default is to load the image into Flash memory.

x Optional. Image is loaded into DRAM without being executed.

destination_ file_name The name of the system image file or the system configuration file. In order for the router to recognize it, the name of the configuration file must be *router_confg*.

Follow these steps to run Xmodem:

Step 1 Move the image file to the local drive where the Xmodem will execute.

Step 2 Enter the **xmodem** command.

Error Reporting

Because the ROM monitor console download uses the console to perform the data transfer, error messages are only displayed on the console when the data transfer is terminated.

If an error does occur during a data transfer, the transfer is terminated, and an error message is displayed. If you have changed the baud rate from the default rate, the error message is followed by a message telling you to restore the terminal to the baud rate specified in the configuration register.

Debug Commands

Most ROM monitor debugging commands are functional only when Cisco IOS software has crashed or is halted. If you enter a debugging command and Cisco IOS crash information is not available, you see the following error message:

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

The following are ROM monitor debugging commands:

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

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

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

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

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

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

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

```
rommon 9> meminfo

Main memory size: 40 MB.
Available main memory starts at 0x10000, size 40896KB
IO (packet) memory size: 5 percent of main memory.
NVRAM size: 32KB
```

Exiting the ROM Monitor

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

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

```
rommon 1 > confreg 0x2101


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

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

Common Port Assignments

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

Table 0-1 Currently Assigned TCP and UDP Port Numbers

Port	Keyword	Description
0	–	Reserved
1–4	–	Unassigned
5	RJE	Remote job entry
7	ECHO	Echo
9	DISCARD	Discard
11	USERS	Active users
13	DAYTIME	Daytime
15	NETSTAT	Who is up or NETSTAT
17	QUOTE	Quote of the day
19	CHARGEN	Character generator
20	FTP-DATA	File Transfer Protocol (data)
21	FTP	File Transfer Protocol
23	TELNET	Terminal connection
25	SMTP	Simple Mail Transport Protocol

Table 0-1 Currently Assigned TCP and UDP Port Numbers (continued)

Port	Keyword	Description
37	TIME	Time
39	RLP	Resource Location Protocol
42	NAMESERVER	Host Name Server
43	NICNAME	Who is
49	LOGIN	Login Host Protocol
53	DOMAIN	Domain Name Server
67	BOOTPS	Bootstrap Protocol Server
68	BOOTPC	Bootstrap Protocol Client
69	TFTP	Trivial File Transfer Protocol
75	–	Any private dial-out service
77	–	Any private RJE service
79	FINGER	Finger
95	SUPDUP	SUPDUP Protocol
101	HOST NAME	NIC host name server
102	ISO-TSAP	ISO-Transport Service Access Point (TSAP)
103	X400	X400
104	X400-SND	X400-SND
111	SUNRPC	SUN Remote Procedure Call
113	AUTH	Authentication Service
117	UUCP-PATH	UNIX-to-UNIX Copy Protocol (UUCP) Path Service
119	NNTP	Usenet Network News Transfer Protocol
123	NTP	Network Time Protocol
126	SNMP	Simple Network Management Protocol
137	NETBIOS-NS	NETBIOS name service

Table 0-1 Currently Assigned TCP and UDP Port Numbers (continued)

Port	Keyword	Description
138	NETBIOS-DGM	NETBIOS datagram service
139	NETBIOS-SSN	NETBIOS session service
161	SNMP	Simple Network Management Protocol Q/R
162	SNMP-TRAP	Simple Network Management Protocol traps
512	rexec	UNIX rexec (control)
513	TCP—rlogin UDP—rwho	TCP—UNIX rlogin UDP—UNIX broadcast name service
514	TCP—rsh UDP—syslog	TCP—UNIX rsh and log
515	Printer	UNIX line printer remote spooling
520	RIP	Routing Information Protocol
525	Timed	Time server

INDEX

Customer Order Number: