

Advanced Features

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

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

Configuring IP EIGRP

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

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

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

Configuring Easy IP (Phase 1)

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

The Easy IP (Phase 1) feature combines NAT and PPP/Internet Protocol Control Protocol (IPCP). With PPP/IPCP, the Cisco 805 router automatically negotiates a globally unique (registered) IP address for the dialer interface from the ISP router. With NAT, the router translates the nonregistered IP addresses used by the LAN devices into the globally unique IP address used by the dialer interface. The ability for multiple LAN devices to use the same globally unique IP address is known as *overloading*. NAT is configured on the router at the border of an *inside network* (a network that uses nonregistered IP addresses) and an *outside network* (a network that uses a globally unique IP address, in this case, the Internet).

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

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

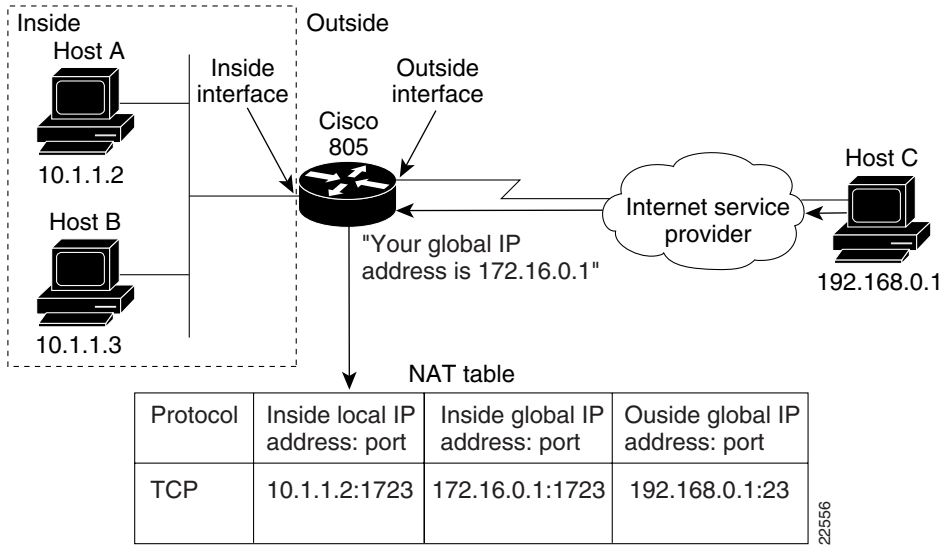
The following is a sample configuration file that contains commands relevant to Easy IP (Phase 1) only:

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

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

- Enables packets having the source address of 10.0.0.0 to 10.255.255.255 to be translated to the globally unique IP address assigned to the router dialer interface and vice versa. The router retains TCP and UDP port numbers of each inside host to translate the global IP address back to the correct local address.
- Establishes the Ethernet interface as an inside interface for NAT.
- Enables PPP/IPCP to automatically negotiate a globally unique IP address for the router dialer interface from the ISP router.
- Establishes the dialer interface as an outside interface for NAT.

Figure 5-1 Easy IP (Phase 1) in Small Office to ISP, Dial-up Line, PPP Sample Network



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

- If the Cisco 805 router does not already have a global IP address for the dialer interface, it requests one from the ISP router.
- The ISP router responds with the global IP address of 172.16.0.1.
- The Cisco 805 router creates a translation that associates the global IP address of the dialer interface (172.16.0.1) with the nonregistered IP address of host A (10.1.1.2). NAT uses the TCP and UDP ports to associate the nonregistered IP address to the global IP address.
- The Cisco 805 router forwards the packet to host C.

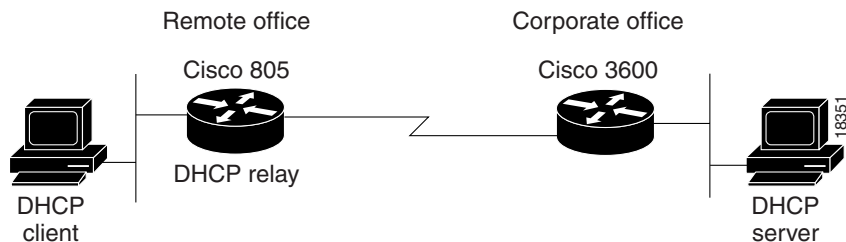
When host C attempts to respond to host A, the Cisco 805 router determines that the global IP address 172.16.0.1 contained in the packet for host A should be translated back to 10.1.1.2. Specifically, the router looks at the inside global IP address and TCP port number (172.16.0.1:1723) in the NAT table and searches for the same TCP port number in the inside local IP address and TCP port number (10.1.1.2:1723).

Configuring Easy IP (Phase 2)

The Easy IP (Phase 2) feature combines DHCP server and relay. With DHCP, LAN devices on an IP network (DHCP clients) can request IP addresses from the DHCP server. The DHCP server allocates IP addresses from a central pool as needed. A DHCP server can be a workstation or PC or a Cisco router. This section explains how to configure the Cisco 805 router as a DHCP server.

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

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



This section explains how to configure the following:

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

DHCP Server

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

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

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

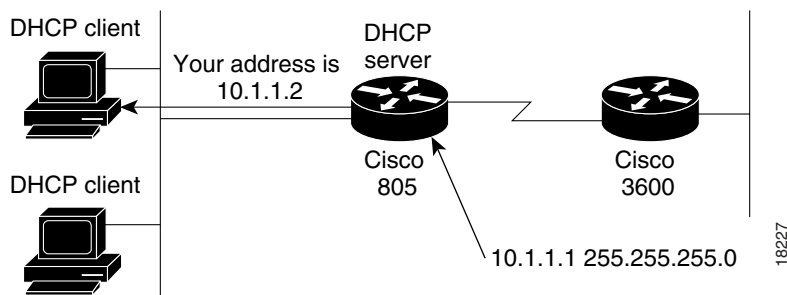
The following is a sample configuration file that contains commands relevant to DHCP server only:

```
!
ip dhcp pool dhcpool_1
network 10.1.1.1 255.255.255.0
default-router 10.1.1.1
!
```

This sample configuration does the following (refer to Figure 5-3):

- Creates a pool (dhcpspool_1) of 254 reusable IP addresses (10.1.1.1 to 10.1.1.254) that can be assigned.
- Designates the Cisco 805 router as the DHCP server to which DHCP clients send their IP address requests and assigns the IP address of 10.1.1.1 to the router.

Figure 5-3 DHCP Server in Remote Office to Corporate Office, Dial-up line, PPP Sample Network



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

DHCP Relay

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

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

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

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

```

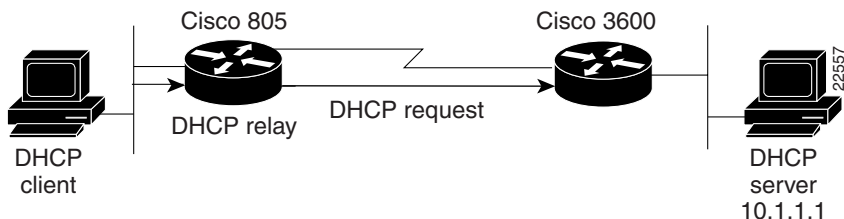
!
ip dhcp-server 10.1.1.1
!
interface serial 0
ip helper-address 10.1.1.1
!

```

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

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

Figure 5-4 DHCP Relay in Remote Office to Corporate Office, Frame Relay Sample Network



Configuring NAT Overload

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

NAT is configured on the router at the border of an *inside network* (a network that uses nonregistered IP addresses) and an *outside network* (a network that uses a globally unique IP address, in this case, the Internet). NAT translates the inside local address (the nonregistered IP address assigned to a host on the inside network) to a globally unique IP address before sending packets to the outside network.

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

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

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

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

```

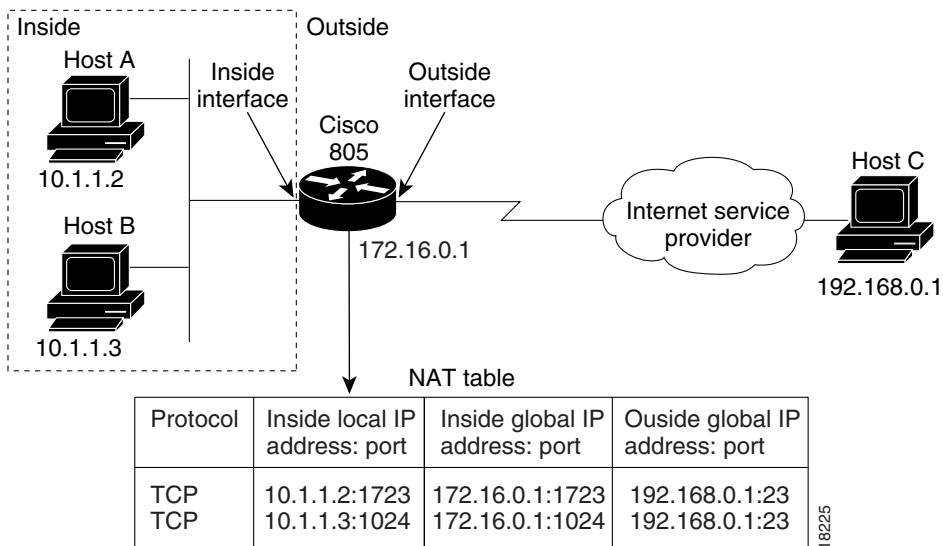
!
interface ethernet 0
ip address 10.1.1.2 255.255.255.0
ip nat inside
!
interface serial 0
ip address 172.16.0.1 255.255.255.0
ip nat outside
!
access list 1 permit 10.0.0.0 0.255.255.255
ip nat inside source list 1 interface serial 0 overload
!

```

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

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

Figure 5-5 NAT in Small Office to ISP, Leased Line, PPP Sample Network



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

- Determines that the IP addresses of host A (10.1.1.2) and host B (10.1.1.3) should be translated to 172.16.0.1.
- Forwards the packets from hosts A and B to host C.

When host C attempts to respond to hosts A and B, the router does the following:

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

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

Configuring the Firewall Feature

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

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

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

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

Configuring Windows NT

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

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

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

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

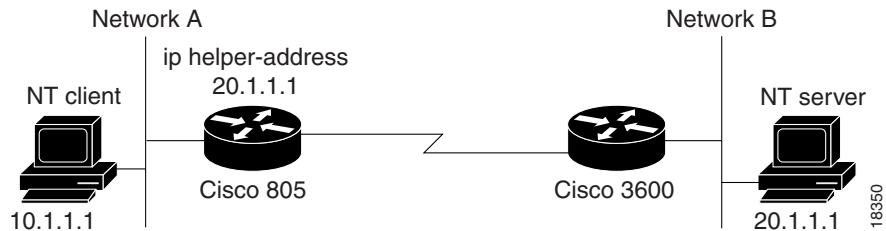
```

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

```

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

Figure 5-6 Cisco 805 Router Forwarding UDP Broadcasts



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

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

Controlling Dial-up Line Activation

This section explains how to control dial-up line activation in Network 4: Dial-up Line, PPP in Chapter 3, “Configuring Remote Office to Corporate Office Networks” and in “Network 2: Dial-up Line, PPP” in Chapter 4, “Configuring Small Office to ISP Networks.”

The following types of traffic can activate your dial-up line and increase your monthly dial-up line cost:

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

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

UDP Broadcasts in a Windows NT Environment

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

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

Configuration

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

Step	Task	Router Prompt	Command
1	Enter configuration mode.	Router#	configure terminal
2	Enter configuration mode for serial interface.	Router (config)#	interface serial 0
3	Create a dialer list.	Router (config-if)#	dialer-group 1
4	Enable interface and configuration changes made to interface.	Router (config-if)#	no shutdown
5	Return to configuration mode.	Router (config-if)#	exit

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

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

UDP Broadcasts in a DHCP Relay Environment

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

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

Controlling Dial-up Line Activation

Configuration

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

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

UDP Broadcasts in an SNTP Environment

You can configure an extended access list so that UDP broadcasts associated with SNTP do not activate the dial-up line.

Configuration

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

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

IP Traffic

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

Controlling Dial-up Line Activation

Configuration

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

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

IPX Traffic

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

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

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

Configuration

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

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

Restricting Access to Your IP Network

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

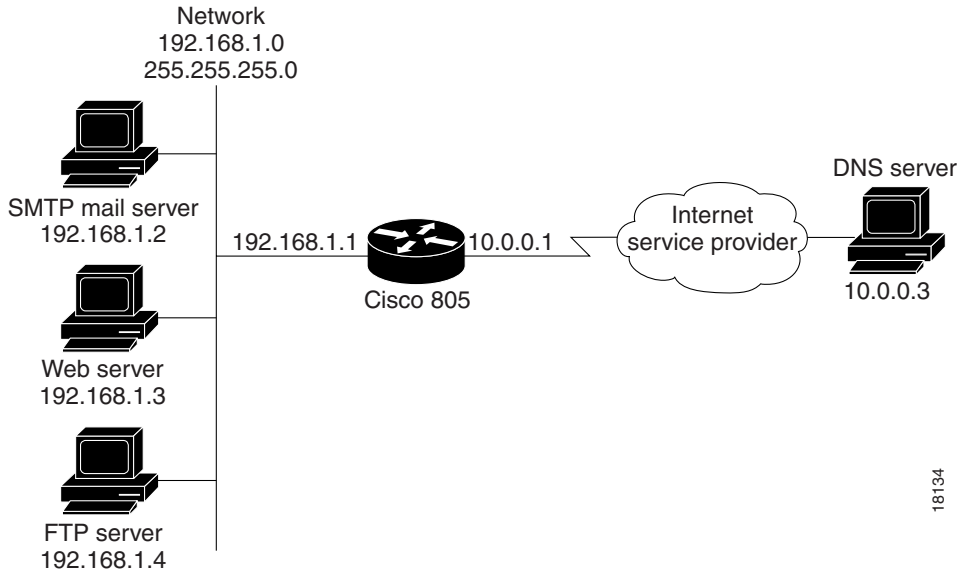
Restricting Access to Your IP Network

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

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

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

Figure 5-7 Restricting Access to IP Network



18134

Table 5-1 Sample IP Network-to-Internet Restrictions

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

Configuration

Use the steps in this table to set up a sample extended access list based on the restrictions in Table 5-1. Use the information in this table as a guideline for setting up your own access list rather than necessarily configuring these settings on your router.

For information on the commands used in this table, refer to the Cisco IOS Release 12.0 documentation set. For information on TCP and UDP port assignments, refer to Appendix F, “Common Port Assignments.”

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

