Configuring Frame Relay

This chapter describes how to configure a Cisco 1600 series router to connect to a central-site router over a a Frame Relay line and provides verification steps and troubleshooting tips.

This chapter contains the following sections:

Before You Begin

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

- Your Cisco 1600 hardware is correctly installed according to the *Cisco 1600 Series Hardware Installation Guide* that came with the router.
- Your Cisco 1600 is connected to a central-site router over Frame Relay.
- Your Cisco 1600 is using multilink Point-to-Point Protocol (PPP).

Before you begin configuration, be aware of the following:

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

Note In order to use the verification steps described in this chapter, you must be familiar with Cisco IOS commands and command modes. When you use the verification steps, you need to change to different command modes. If you are not familiar with command modes, refer to the "Understanding Command Modes" section in the "Cisco IOS Basic Skills" chapter.

Frame Relay

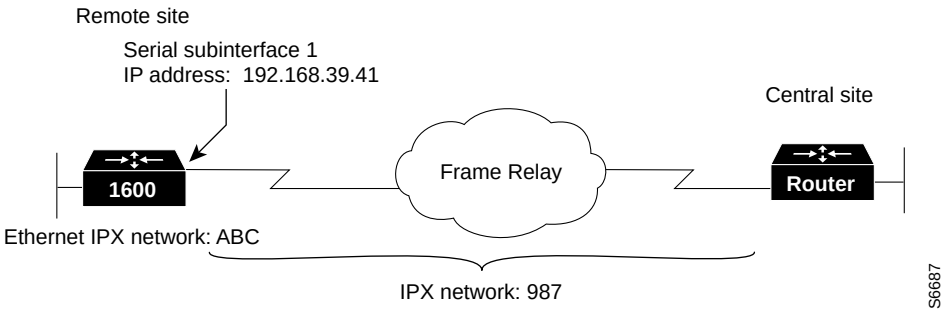
This section describes how to configure a basic Frame Relay connection to the central-site router.

These are the major tasks when configuring your router:

- Configuring Global Parameters
- Configuring Security
- Configuring the Ethernet Interface
- Configuring the Serial Interface for a Frame Relay Connection
- Configuring the Point-to-Point Frame Relay Connection
- Configuring Routing Parameters
- Configuring Command Line Access to the Router

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

Figure 5-1 Frame Relay Example Configuration



Configuring Global Parameters

Use this table to configure the router for some global parameters, including the default domain name that the router uses, the server used by the router to find out its name and IP address, and enabling IPX routing.

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

Configuring Security

Use this table to configure the router with some security measures, such as the router host name and the password used to prevent unauthorized access to the router.

		Prompt	Command
Step 1	Configure the router with a host name, which is used in prompts and default configuration file names. For PPP authentication, the host name entered with this command must match the username of the central-site router.	`Router(config)#`	**`hostname`** *`1600`*
Step 2	Specify a password to prevent unauthorized access to the router.	`1600(config)#`	**`enable password`** *`1600user`*

Configuring the Ethernet Interface

Use this table to configure the Ethernet interface (which connects the router to your local network) for IP and IPX routing and network addresses.

		Prompt	Command
Step 1	Enter configuration mode for the Ethernet interface.	`1600(config)#`	`interface Ethernet0`
Step 2	Configure this interface with an IP address and a subnet mask.	`1600(config-if)#`	**`ip address`** *`172.16.25.1 255.255.255.0`*
Step 3	Enable IPX routing on this interface.	`1600(config-if)#`	**`ipx network`** *`ABC`*
Step 4	Enable the interface and the configuration changes that you have just made on the interface.	`1600(config-if)#`	`no shutdown`
Step 5	Exit configuration mode for this interface.	`1600(config-if)#`	`exit`

Configuring the Serial Interface for a Frame Relay Connection

Use this table to configure the serial interface for Frame Relay packet encapsulation.

		Router Prompt	Command
Step 1	Enter configuration mode for the serial interface.	`1600(config)#`	`interface Serial0`
Step 2	Set the encapsulation method on this interface to Frame Relay.	`1600(config-if)#`	`encapsulation frame-relay`
Step 3	Enable the configuration changes on this interface.	`1600(config-if)#`	`no shutdown`

Verifying Your Configuration

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

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

Step 2 From the privileged EXEC command mode, enter the **show frame-relay pvc** command.

Step 3 Confirm that the "PVC STATUS=ACTIVE" message (shown in bold in the example) appears in the command output:

```
1600# show frame-relay pvc

PVC Statistics for interface Serial0 (Frame Relay DTE)

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

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

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

Step 5 If there is no output after entering the command, use the **show interface serial0** command to determine whether or not the serial interface is active. An example of this command is in the next section, "Configuring the Point-to-Point Frame Relay Connection." The first line of the command output should be this:

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

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

Step 6 To continue configuration, re-enter global configuration mode.

Configuring the Point-to-Point Frame Relay Connection

Use this table to configure the Frame Relay interface to send IP and IPX data to the central-site router over a point-to-point connection.

		Prompt	Command
Step 1	Enter configuration mode for the serial subinterface and specify this interface as a point-to-point connection.	`1600(config-if)#`	`interface Serial0.1 point-to-point`
Step 2	Configure this interface with an IP address and a subnet mask.	`1600(config-if)#`	**`ip address`** *`192.168.39.40 255.255.255.0`*
Step 3	Enable IPX routing on this interface.	`1600(config-if)#`	**`ipx network`** *`987`*
Step 4	Assign a data link connection identifier (DLCI) to the Frame Relay subinterface. If you are unsure of the DLCI, use the number that you recorded in Step 4 of the previous "Verifying Your Configuration" section.	`1600(config-if)#`	**`frame-relay interface-dlci`** *`17`*

		Prompt	Command
Step 5	Enable snapshot routing. Because your router is dialing into a central-site router, it is considered the client router. The first number is the amount of "active time" (in minutes) during which routing updates are exchanged between your router and the central-site router. The second number is the amount of "quiet time" (in minutes) during which routing entries are frozen and remain unchanged.	`1600(config-if)#`	**`snapshot client`** *`5 60`*
Step 6	Enable the interface and the configuration changes that you have just made on the interface.	`1600(config-if)#`	`no shutdown`
Step 7	Exit configuration mode for this interface.	`1600(config-if)#`	`exit`

Verifying Your Configuration

You can verify your configuration to this point by

- Confirming that the Line Is Up.
- Confirming the Frame Relay Maps.
- Confirming Connectivity to the Central-Site Router.

Confirming that the Line Is Up

Step 1 From the privileged EXEC command mode, enter the **show interface serial 0** command, as follows:

```
1600# show interfaces serial 0

Serial0 is up, line protocol is up
  Hardware is QUICC Serial
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load
1/255
  Encapsulation FRAME-RELAY, loopback not set, keepalive set (10 sec)
  LMI enq sent  163, LMI stat recvd 136, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 39, LMI stat sent  0, LMI upd sent  0
  LMI DLCI 1023  LMI type is CISCO  frame relay DTE
```

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

Step 2 Confirm that the following messages (shown in bold) appear in the command output:

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

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

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

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

Step 4 To continue configuration, re-enter global configuration mode.

Confirming the Frame Relay Maps

Step 1 From the privileged EXEC command mode, enter the **show frame-relay map** command.

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

```
1600# show frame-relay map
Serial0.1 (up): point-to-point dlci, dlci 17(0x11,0x410), broadcast,
          status defined, active
```

Step 3 If the message does not appear, confirm that

a. The central-site router is connected and configured.

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

Step 4 To continue configuration, re-enter global configuration mode.

Confirming Connectivity to the Central-Site Router

Step 1 From the privileged EXEC command mode, enter the **ping** command followed by the IP address of the central-site router.

Step 2 Note the percentage in the "Success rate..." line (shown in bold in the example):

```
1600# ping 192.168.38.40

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.38.40, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32
ms
1600#
```

If the success rate is 10 percent or greater, this verification step is successful.

Step 3 To continue configuration, re-enter global configuration mode.

Configuring Routing Parameters

Use this table to configure the Frame Relay interface for Enhanced Interior Gateway Routing Protocol (EIGRP) routing.

		Prompt	Command
Step 1	Configure the IP EIGRP routing process.	`1600(config)#`	**router eigrp** *202*
Step 2	Specify a list of networks for the EIGRP routing process by entering the IP address of the directly connected network.	`1600(config-router)#`	**network** *172.16.0.0*
Step 3	Configure the router to forward packets addressed to a subnet of a network with no network default route.	`1600(config-router)#`	`ip classless`
Step 4	Exit router configuration mode.	`1600(config-router)#`	`exit`

Configuring Command Line Access to the Router

Use this table to configure some parameters that control access to the router, including the type of terminal line used with the router, how long the router waits for a user entry before it times out, and the password used to start a terminal session with the router.

		Prompt	Command
Step 1	Specify the console terminal line.	`1600(config)#`	**line console** *0*
Step 2	Set the interval that the EXEC command interpreter waits until user input is detected.	`1600(config-line)#`	**exec-timeout** *5*
Step 3	Specify a virtual terminal for remote console access.	`1600(config-line)#`	**line vty** *0 4*
Step 4	Specify a password on the line.	`1600(config-line)#`	**password** *lineaccess*

		Prompt	Command
Step 5	Enable password checking at terminal session login.	`1600(config-line)#`	**`login`**
Step 6	Exit configuration mode.	`1600(config-line)#`	`end`

Frame Relay with an Internal DSU/CSU

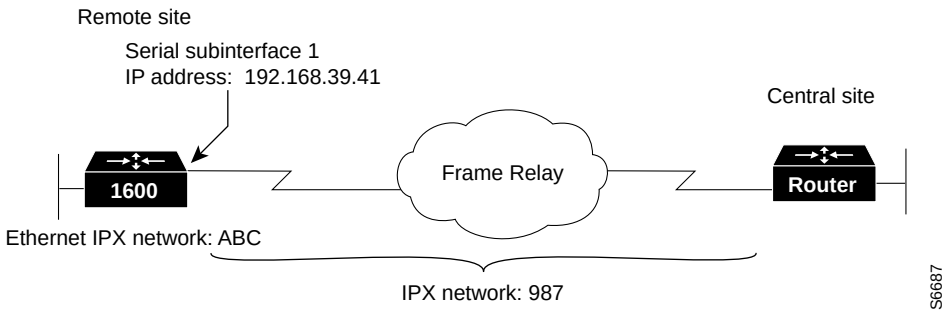
This section describes how to configure a a Cisco 1600 with an internal data service unit/channel service unit (DSU/CSU) for Frame Relay. In addition to the assumptions described in the "Before You Begin" section of this chapter, this configuration assumes that the internal DSU/CSU is a switched 56-kbps interface.

These are the major tasks when configuring your router:

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

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

Figure 5-2 Frame Relay Internal DSU/CSU Example Configuration



Configuring Global Parameters

Use this table to configure the router for some global parameters, including the ISDN switch type that the router connects to through the ISDN line and how log and debug messages are timestamped.

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

Configuring Security

Use this table to configure the router with some security measures, such as the router host name and the password used to prevent unauthorized access to the router.

		Prompt	Command
Step 1	Configure the router with a host name, which is used in prompts and default configuration file names. For PPP authentication, the host name entered with this command must match the username of the central-site router.	`Router(config)#`	**hostname** *1600*
Step 2	Specify a password to prevent unauthorized access to the router.	`1600(config)#`	**enable password** *1600user*

Configuring the Ethernet Interface

Use this table to configure the Ethernet interface (which connects the router to your local network) for IP and IPX routing, including configuring network addresses.

		Prompt	Command
Step 1	Enter configuration mode for the Ethernet interface.	`1600(config)#`	`interface Ethernet0`
Step 2	Configure this interface with an IP address and a subnet mask.	`1600(config-if)#`	**ip address** *172.16.25.1 255.255.255.224*
Step 3	Enable IPX routing on this interface.	`1600(config-if)#`	**ipx network** *ABC*
Step 4	Enable the interface and the configuration changes that you have just made on the interface.	`1600(config-if)#`	`no shutdown`
Step 5	Exit configuration mode for this interface.	`1600(config-if)#`	`exit`

Configuring the Frame Relay Interface

Use this table to configure the serial interface for Frame Relay packet encapsulation and for an internal DSU/CSU.

		Prompt	Command
Step 1	Enter configuration mode for the serial interface.	`1600(config)#`	`interface Serial0`
Step 2	Disable IP routing on this interface.	`1600(config-if)#`	`no ip address`
Step 3	Set the encapsulation method on this interface to Frame Relay.	`1600(config-if)#`	`encapsulation frame-relay`
Step 4	Configure the clock source for the 56-kbps DSU/CSU module. In most applications, the DSU/CSU should be configured with the **clock source line** command. For back-to-back DSU/CSU configurations, configure one DSU/CSU with the **clock source internal** command and the other with **clock source line** command.	`1600(config-if)#`	`service-module 56k clock source line`
Step 5	Configure this interface to transmit packets in switched dial-up mode or digital data service mode using the 56-kbps DSU/CSU module. If the clock rate has not been set correctly with the **service-module 56k clock source line** command, this command is not accepted by the router.	`1600(config-if)#`	`service-module 56k network type dds`

Verifying Your Configuration

You can verify your configuration to this point by

- Confirming that the Line Is Up.
- Confirming that the Interface Is Receiving a Line Signal.

Confirming that the Line Is Up

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

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

```
1600# show interfaces serial 0
Serial0 is up, line protocol is up
  Hardware is QUICC Serial
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load
1/255
  Encapsulation FRAME-RELAY, loopback not set, keepalive set (10 sec)
  LMI enq sent  163, LMI stat recvd 136, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 39, LMI stat sent  0, LMI upd sent  0
  LMI DLCI 1023  LMI type is CISCO  frame relay DTE
  Broadcast queue 0/64, broadcasts sent/dropped 27/0, interface
broadcasts 28
  Last input 00:00:01, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/64/0 (size/threshold/drops)
     Conversations  0/1 (active/max active)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1813 packets input, 109641 bytes, 0 no buffer
     Received 1576 broadcasts, 0 runts, 0 giants
     13 input errors, 0 CRC, 13 frame, 0 overrun, 0 ignored, 0 abort
     1848 packets output, 117260 bytes, 0 underruns
     0 output errors, 0 collisions, 32 interface resets
     0 output buffer failures, 0 output buffers swapped out
     29 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Step 3 To continue configuration, re-enter global configuration mode.

Confirming that the Interface Is Receiving a Line Signal

Step 1 From the privileged EXEC command mode, enter the **show service module serial 0** command:

```
1600# show service-module serial 0
Module type is 4-wire Switched 56K in DDS mode,
Current line rate is 56 Kbits/sec and role is Telco side,
Last clearing of alarm counters 21:23:25
    oos/oof                :    0,
    loss of signal       :   0,
    loss of sealing current:    0,
    CSU/DSU loopback       :    0,
    loopback from remote   :    0,
    DTE loopback           :    0,
    line loopback          :    0,
```

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

Step 3 To continue configuration, re-enter global configuration mode.

Configuring the Frame Relay Subinterface

Use this table to configure the Frame Relay subinterface for IP and IPX routing, including network addresses, and to assign a data link connection identifier (DLCI) to the interface.

		Prompt	Command
Step 1	Enter configuration mode for the serial subinterface and specify this interface as a point-to-point connection.	`1600(config-if)#`	`interface Serial0.1 point-to-point`
Step 2	Configure this interface with an IP address and a subnet mask.	`1600(config-if)#`	**ip address** *172.16.26.1 255.255.255.0*
Step 3	Enable IPX routing on this interface.	`1600(config-if)#`	**ipx network** *987*

		Prompt	Command
Step 4	Assign a DLCI to the Frame Relay subinterface.	`1600(config-if)#`	**frame-relay interface-dlci** *17*
Step 5	Configure this interface with an IP address and a subnet mask.	`1600(config-if)#`	**ip address** *192.168.38.41 255.255.255.0*
Step 6	Enable IPX routing on this interface.	`1600(config-if)#`	**ipx network** *456*
Step 7	Enable snapshot routing. Because your router is dialing into a central-site router, it is considered the client router. The first number is the amount of "active time" (in minutes) during which routing updates are exchanged between your router and the central-site router. The second number is the amount of "quiet time" (in minutes) during which routing entries are frozen and remain unchanged.	`1600(config-if)#`	**snapshot client** *5 60*
Step 8	Assign a DLCI to the Frame Relay subinterface.	`1600(config-if)#`	**frame-relay interface-dlci** *17*
Step 9	Enable the interface and the configuration changes that you have just made on the interface.	`1600(config-if)#`	`no shutdown`
Step 10	Exit configuration mode for the serial interface.	`1600(config-if)#`	`exit`

Configuring Routing Parameters

Use this table to configure the Frame Relay interface for Enhanced Interior Gateway Routing Protocol (EIGRP) routing.

		Prompt	Command
Step 1	Configure the IP EIGRP routing process.	`1600(config)#`	**router eigrp** *202*
Step 2	Specify a list of networks for the EIGRP routing process by entering the IP address of the directly connected network.	`1600(config-router)#`	**network** *172.16.0.0*

		Prompt	Command
Step 3	Configure the router to forward packets addressed to a subnet of a network with no network default route.	`1600(config-router)#`	`ip classless`
Step 4	Exit router configuration mode.	`1600(config-router)#`	`exit`

Configuring Command Line Access to the Router

Use this table to configure some parameters that control access to the router, including what type of terminal line can be used with the router, how long the user has to input a command before the router times out, and the password used to start a terminal session with the router.

		Prompt	Command
Step 1	Specify the console terminal line.	`1600(config)#`	**line console** *0*
Step 2	Set the interval that the EXEC command interpreter waits until user input is detected.	`1600(config-line)#`	**exec-timeout** *5*
Step 3	Specify a virtual terminal for remote console access.	`1600(config-line)#`	**line vty** *0 4*
Step 4	Specify a password on the line.	`1600(config-line)#`	**password** *lineaccess*
Step 5	Enable password checking at terminal session login.	`1600(config-line)#`	**login**
Step 6	Exit configuration mode.	`1600(config-line)#`	`end`

ISDN as the Backup WAN Connection

This section describes how to configure ISDN to operate as a secondary, or backup, WAN connection. You do this so that the router continues to operate if the main WAN connection is down. This configuration is usually used on an ISDN WAN interface card that is installed in a Cisco 1600 router. The router on-board WAN port is the primary, or main, WAN connection, and the card WAN port is the secondary connection.

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

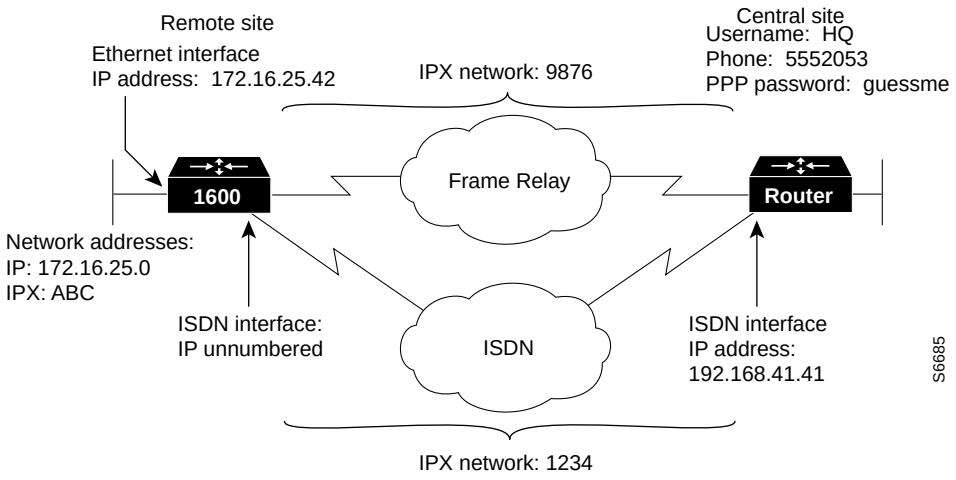
- Frame Relay is used as the primary WAN connection to the central site.
- The ISDN line is used as the secondary WAN connection to the central site.

These are the major tasks when configuring your router:

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

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

Figure 5-3 ISDN as Backup Connection Example Configuration



Configuring Global Parameters

Use this table to configure the router for some global parameters, including the ISDN switch type that the router is connected to through the ISDN line, how log and debug messages are timestamped, and the router IPX address.

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

		Prompt	Command
Step 5	Configure the type of central office switch being used on the ISDN interface. Use the keyword that matches the ISDN switch type that you are using: • **basic-ts013** —Australian TS013 switches • **basic-1tr6** —German 1TR6 ISDN switches • **basic-nwnet3**—Norway NET3 switches (phase 1) • **basic-net3**—NET3 ISDN switches • **vn2**—French VN2 ISDN switches • **vn3**—French VN3 ISDN switches • **ntt**—Japanese NTT ISDN switches • **basic-5ess**—AT&T basic rate switches • **basic-dms100**—NT DMS-100 basic rate switches • **basic-ni1**—National ISDN-1 switches • **basic-nznet3**—New Zealand Net3 switches	`Router(config)#`	**`isdn switch-type`** *`basic-ni1`*

Configuring Security

Use this table to configure the router with some security measures, such as the router host name, password used to prevent unauthorized access to the router, and the username and password for Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) authentication with the central-site router.

		Prompt	Command
Step 1	Configure the router with a host name, which is used in prompts and default configuration file names. For PPP authentication, the host name entered with this command must match the username of the central-site router.	`Router(config)#`	**`hostname`** *`1600`*

		Prompt	Command
Step 2	Specify a password to prevent unauthorized access to the router.	`1600(config)#`	**enable password** *1600user*
Step 3	Specify the password used during caller identification and CHAP and PAP authentication. For CHAP and PAP authentication, the username entered with this command must match the host name of the central-site router.	`1600(config)#`	**username** *HQ* **password** *guessme*

Configuring the Ethernet Interface

Use this table to configure the Ethernet interface for IP and IPX routing and network addresses.

		Prompt	Command
Step 1	Enter configuration mode for the Ethernet interface.	1600(config)#	interface Ethernet0
Step 2	Configure this interface with an IP address and a subnet mask.	1600(config-if)#	**ip address** *172.16.25.1 255.255.255.0*
Step 3	Configure the Ethernet interface IPX network number.	1600(config-if)#	ipx network *ABC*
Step 4	Enable the interface and the configuration changes that you have just made on the interface.	1600(config-if)#	no shutdown
Step 5	Exit configuration mode for the this interface.	1600(config-if)#	exit

Configuring the Frame Relay Interface

Use this table to configure the Frame Relay interface for the following:

- A point-to-point connection to the central-site router
- The ISDN used as a backup connection for the serial connection
- IP and IPX routing parameters
- The DLCI identifier to the Frame Relay line used on this interface

		Prompt	Command
Step 1	Enter configuration mode for the serial interface.	`1600(config)#`	`interface Serial0`
Step 2	Set the encapsulation method on this interface to Frame Relay.	`1600(config-if)#`	`encapsulation frame-relay`
Step 3	Enter configuration mode for the serial subinterface and specify this interface as a point-to-point connection.	`1600(config-if)#`	`interface Serial0.1 point-to-point`
Step 4	Configure the BRI interface to act as a backup line for this interface.	`1600(config-if)#`	`backup interface BRI0`
Step 5	Define when the ISDN line is used as a backup for this interface: • The first number is how many seconds the Frame Relay line is down before the ISDN line comes up as the backup line. • The second number is how many seconds after the Frame Relay line comes back up until the ISDN line goes down.	`1600(config-if)#`	**`backup delay`** *`10 10`*
Step 6	Configure this interface with an IP address.	`1600(config-if)#`	**`ip address`** *`172.16.26.1 255.255.255.0`*
Step 7	Enable IPX routing on this interface.	`1600(config-if)#`	**`ipx network`** *`9876`*
Step 8	Assign a data link connection identifier (DLCI) to the Frame Relay subinterface.	`1600(config-if)#`	**`frame-relay interface-dlci`** *`17`*
Step 9	Enable the interface and the configuration changes that you have just made on the interface.	`1600(config-if)#`	`no shutdown`
Step 10	Exit configuration mode for this interface.	`1600(config-if)#`	`exit`

Configuring the ISDN Interface

Use this table to configure the ISDN line to act as a backup connection, if for some reason the Frame Relay connection goes down.

		Router Prompt	Command
Step 1	Enter configuration mode for the ISDN interface.	1600(config)#	interface BRI0
Step 2	Define the service profile identifier (SPID) number assigned by the ISDN service provider to the B1 channel. This step is required only when the service provider has assigned a SPID to your ISDN line. Not all ISDN lines have SPIDs.	1600(config-if)#	**isdn spid1** *555987601*
Step 3	Define the SPID number assigned by the ISDN service provider to the B2 channel. This step is required only when the service provider has assigned a SPID to your ISDN line. Not all ISDN lines have SPIDs.	1600(config-if)#	**isdn spid2** *555987602*
Step 4	Enable IP routing on the this interface without assigning an IP address.	1600(config-if)#	ip unnumbered Ethernet0
Step 5	Define the IPX network number for this interface.	1600(config-if)#	ipx network *1234*
Step 6	Set the encapsulation method on this interface to PPP.	1600(config-if)#	encapsulation ppp
Step 7	Specify the telephone number that this interface dials to connect to the central-site router. This command is used when the interface is only connecting to a single remote site.	1600(config-if)#	**dialer string** *5552053*
Step 8	Assign this interface to a dialer group.	1600(config-if)#	**dialer-group** *1*
Step 9	Enable CHAP and PAP authentication on this interface. CHAP authentication is attempted first. If the central-site router does not support CHAP, PAP is used for authentication.	1600(config-if)#	ppp authentication chap pap callin
Step 10	Enable multilink PPP on this interface.	1600(config-if)#	ppp multilink
Step 11	Enable the interface and the configuration changes that you have just made on the interface.	1600(config-if)#	no shutdown
Step 12	Exit configuration mode for this interface.	1600(config-if)#	exit

Verifying Your Configuration

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

Step 1 From the privileged EXEC command mode, enter the **ping** command followed by the IP address of the central-site router:

```
1600# ping 192.168.37.40

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.37.40, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 40/43/48 ms
1600#
*Mar  1 03:37:46.526: %LINK-3-UPDOWN: Interface BRI0:1, changed state
to up
*Mar  1 03:37:46.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface
BRI0:1, changed state to up
*Mar  1 03:37:46.939: %LINK-3-UPDOWN: Interface Virtual-Access1,
changed state to up
*Mar  1 03:37:47.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access1, changed state to up
 *Mar  1 03:35:57.217: %ISDN-6-CONNECT: Interface BRI0:1 is now
connected to 5552053 HQ
```

Step 2 Note the percentage in the "Success rate..." line (shown in bold in the example). If the success rate is 60 percent (3/5) or greater, your router is successfully transferring date to the central-site router.

Step 3 If the success rate is less than 60 percent, take the following steps:

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

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

Step 4 To continue configuration, re-enter global configuration mode.

Configuring Protocols and Dialing Behavior

Use this table to configure types of network data that causes your router to dial to the central-site router.

		Prompt	Command
Step 1	Configure the IP Enhanced Interior Gateway Routing Protocol (EIGRP) routing process.	1600(config)#	**router eigrp** *202*
Step 2	Specify a list of networks for the EIGRP routing process by entering the IP address of the directly connected network.	1600(config-router)#	**network** *172.16.0.0*
Step 3	Specify that the router does not forward packets that are destined for a subnet of a network that has no network default route.	1600(config-router)#	ip classless
Step 4	Specify an access list by list number and protocol (IP) to define the "interesting" packets that can trigger a called to the destination.	1600(config-router)#	**dialer-list** *1* **protocol ip permit**
Step 5	Specify an access list by list number and protocol (IPX) to define the "interesting" packets that can trigger a called to the destination.	1600(config-router)#	**dialer-list** *1* **protocol ipx permit**
Step 6	Exit router configuration mode.	1600(config-router)#	exit

Configuring Command Line Access to the Router

Use this table to configure some parameters that control access to the router, including the type of terminal line used with the router, how long the router waits for a user entry before it times out, and the password used to start a terminal session with the router.

		Prompt	Command
Step 1	Specify the console terminal line.	`1600(config)#`	**`line console`** *`0`*
Step 2	Set the interval that the EXEC command interpreter waits until user input is detected.	`1600(config-line)#`	**`exec-timeout`** *`5`*

		Prompt	Command
Step 3	Specify a virtual terminal for remote console access.	`1600(config-line)#`	**line vty** *0 4*
Step 4	Specify a password on the line.	`1600(config-line)#`	**password** *lineaccess*
Step 5	Enable password checking at terminal session login.	`1600(config-line)#`	**login**
Step 6	Exit configuration mode.	`1600(config-line)#`	`end`

Verifying Your Configuration

You can verify your router configuration to this point by confirming that the ISDN connects dynamically to the remote site when the Frame Relay connection is disconnected by taking the following steps:

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

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

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

Troubleshooting Problems with ISDN as Frame Relay Backup Line

If you are having problems, take some or all of the following steps:

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

2. If you want to use the ISDN line even when the Frame Relay line is connected, use dialer profiles. Otherwise, the ISDN line operates in backup mode only.
3. If you are still having problems, you can use some or all of the following **debug** commands:

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

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

ISDN as a Backup Connection with Dialer Profiles

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

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

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

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

These are the major tasks when configuring your router:

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

Configuring Global Parameters

Use this table to configure the router for some global parameters, including the ISDN switch type that the router is connected to through the ISDN line, and how log and debug messages are timestamped.

		Prompt	Command
Step 1	Enter configuration mode.	`Router#`	`configure terminal`
Step 2	Configure the router to show the date and time of all debug messages. This command is optional, but recommended if you use debug commands to troubleshoot your configuration.	`Router(config)#`	`service timestamps debug datetime msec`

		Prompt	Command
Step 3	Configure the router to show the date and time of all log messages. This command is optional, but recommended if you use the verification steps described in this guide. This feature is enabled for all the example command output shown in this guide.	`Router(config)#`	`service timestamps log datetime msec`
Step 4	Configure the type of central office switch being used on the ISDN interface. Use the keyword that matches the ISDN switch type that you are using: • **basic-ts013** —Australian TS013 switches • **basic-1tr6** —German 1TR6 ISDN switches • **basic-nwnet3**—Norway NET3 switches (phase 1) • **basic-net3**—NET3 ISDN switches • **vn2**—French VN2 ISDN switches • **vn3**—French VN3 ISDN switches • **ntt**—Japanese NTT ISDN switches • **basic-5ess**—AT&T basic rate switches • **basic-dms100**—NT DMS-100 basic rate switches • **basic-ni1**—National ISDN-1 switches • **basic-nznet3**—New Zealand Net3 switches	`Router(config)#`	*`basic-ni1`*

Configuring Security

Use this table to configure the router with some security measures, the router host name, the password used to prevent unauthorized access to the router, and the username and password that are used for PPP authentication.

		Prompt	Command
Step 1	Configure the router with a host name, which is used in prompts and default configuration file names. For PPP authentication, the host name entered with this command must match the username of the central-site router.	`Router(config)#`	**hostname** *1600*
Step 2	Specify a password to prevent unauthorized access to the router.	`1600(config)#`	**enable password** *1600user*
Step 3	Specify the password used during caller identification and CHAP and PAP authentication. This password applies only to one of the central-site router. For security reasons, a different password should be used for each remote location that the router dials on the backup ISDN line. For PPP authentication, the username entered with this command must match the host name of the central-site router.	`1600(config)#`	**username** *HQ1* **password** *guessme1*
Step 4	Specify the password used during caller identification and CHAP and PAP authentication. This password applies only to one of the central-site router. For security reasons, a different password should be used for each remote location that the router dials on the backup ISDN line. For PPP authentication, the username entered with this command must match the host name of the central-site router.	`1600(config)#`	**username** *HQ2* **password** *guessme2*

Configuring the Ethernet Interface

Use this table to configure the Ethernet interface with an IP address and disable fast and autonomous switching.

		Prompt	Command
Step 1	Enter configuration mode for this interface.	`1600(config)#`	`interface ethernet0`
Step 2	Configure this interface with an Ethernet address.	`1600(config-if)#`	**`ip address`** *`172.16.20.1 255.255.255.0`*
Step 3	Disable fast switching and autonomous switching on this interface.	`1600(config-if)#`	`no ip route-cache`
Step 4	Enable IP multicast fast switching on this interface.	`1600(config-if)#`	`ip mroute-cache`
Step 5	Enable the configuration changes for this interface.	`1600(config-if)#`	`no shutdown`
Step 6	Exit configuration mode for this interface.	`1600(config-if)#`	`exit`

Configuring the Serial Interface

Use this table to configure the serial interface for Frame Relay.

		Prompt	Command
Step 1	Enter configuration mode for this interface.	`1600(config)#`	`interface serial0`
Step 2	Disable IP processing for this interface.	`1600(config-if)#`	`no ip address`
Step 3	Configure this interface for Frame Relay encapsulation.	`1600(config-if)#`	`encapsulation frame-relay`
Step 4	Enable the configuration changes for this interface.	`1600(config-if)#`	`no shutdown`
Step 5	Exit configuration mode for this interface.	`1600(config-if)#`	`exit`

Configuring the Primary Connection to the First Central-Site Router

Use this table to configure a point-to-point Frame Relay connection to one of the central-site routers that your router connects to.

		Prompt	Command
Step 1	Create a subinterface and enter configuration mode for the interface.	`1600(config)#`	`interface serial0.1 point-to-point`
Step 2	Define when the ISDN line is used as a backup for this interface: • The first number is how many seconds the Frame Relay line is down before the ISDN line comes up as the backup line. • The second number is how many seconds after the Frame Relay line comes back up until the ISDN line goes down.	`1600(config-if)#`	**`backup delay`** *`10 10`*
Step 3	Configure the BRI interface to act as a dial backup line for this subinterface.	`1600(config-if)#`	`backup interface Dialer1`
Step 4	Configure this subinterface with an IP address.	`1600(config-if)#`	`ip address` *`172.16.30.40 255.255.255.0`*
Step 5	Configure this subinterface with an IPX network address.	`1600(config-if)#`	`ipx network` *`AABB`*
Step 6	Assign a data link connection identifier (DLCI) to this subinterface.	`1600(config-if)#`	**`frame-relay interface-dlci`** *`17`*
Step 7	Enable the configuration changes for this subinterface.	`1600(config-if)#`	`no shutdown`
Step 8	Exit configuration mode for this subinterface.	`1600(config-if)#`	`exit`

Configuring the Primary Connection to the Second Central-Site Router

Use this table to configure a point-to-point Frame Relay connection to one of the central-site routers that your router connects to.

		Prompt	Command
Step 1	Create a subinterface and enter configuration mode for the interface.	`1600(config)#`	`interface serial0.2 point-to-point`
Step 2	Define when the ISDN line is used as a backup for this interface: • The first number is how many seconds the Frame Relay line is down before the ISDN line comes up as the backup line. • The second number is how many seconds after the Frame Relay line comes back up until the ISDN line goes down.	`1600(config-if)#`	**backup delay** *10 10*
Step 3	Configure the BRI interface to act as a dial backup line for this subinterface.	`1600(config-if)#`	`backup interface Dialer2`
Step 4	Configure this subinterface with an IP address.	`1600(config-if)#`	`ip address` *172.16.40.40 255.255.255.0*
Step 5	Configure this subinterface with an IPX network address.	`1600(config-if)#`	`ipx network` *BBCC*
Step 6	Assign a data link connection identifier (DLCI) to this subinterface.	`1600(config-if)#`	**frame-relay interface-dlci** *18*
Step 7	Enable the configuration changes for this subinterface.	`1600(config-if)#`	`no shutdown`
Step 8	Exit configuration mode for this subinterface.	`1600(config-if)#`	`exit`

Configuring the ISDN Interface

Use this table to configure the ISDN interface for PPP packet encapsulation and to assign it to a dialer pool.

		Prompt	Command
Step 1	Enter configuration mode for this interface.	`1600(config)#`	`interface BRI0`
Step 2	Configure this interface for PPP packet encapsulation.	`1600(config-if)#`	`encapsulation ppp`
Step 3	Assign this interface to a dialer pool.	`1600(config-if)#`	`dialer pool-member` *`1`*
Step 4	Enable the configuration changes on this interface.	`1600(config-if)#`	`no shutdown`
Step 5	Exit configuration mode for this interface.	`1600(config-if)#`	`exit`

Configuring the Backup Connection to the First Central-Site Router

Use this table to configure the backup connection to the first central-site router, including packet encapsulation, network addresses, authentication method, and the number that the router dials to connect to the central-site router.

		Prompt	Command
Step 1	Create an ISDN dialer interface, and enter configuration mode for the interface. The number that you assign in this command must match the number you assigned with the **backup interface** command when you configured the primary connection to the first central-site router.	1600(config)#	interface Dialer1
Step 2	Enable IP routing without assigning an IP address.	1600(config-if)#	ip unnumbered ethernet0

		Prompt	Command
Step 3	Configure this interface for PPP packet encapsulation.	1600(config-if)#	encapsulation ppp
Step 4	Configure this interface with an IPX network number.	`1600(config-if)#`	`ipx network` *`DCBA`*
Step 5	Configure the name of the central-site router that this interface dials. The name that you enter with this command should be the same name that you entered with the **username password** command in the "Configuring Security" section.	`1600(config-if)#`	`dialer remote-name` *`HQ1`*
Step 6	Configure the number that the interface dials to connect to the central-site router.	`1600(config-if)#`	`dialer string` *`5551234`*
Step 7	Specify that the router can have only one call connected to the first central-site router at any one time.	`1600(config-if)#`	`dialer max-call 1`
Step 8	Assign this interface to a dialer pool.	`1600(config-if)#`	`dialer pool` *`1`*
Step 9	Assign this interface to a dialer group.	`1600(config-if)#`	`dialer-group` *`1`*
Step 10	Specify that CHAP authentication is performed when this interface connects to the central-site router.	`1600(config-if)#`	`ppp authentication chap`
Step 11	Enable the configuration changes for this interface.	`1600(config-if)#`	`no shutdown`
Step 12	Exit configuration mode for this subinterface.	`1600(config-if)#`	`exit`

Configuring the Backup Connection to the Second Central-Site Router

Use this table to configure the backup connection to the first central-site router, including packet encapsulation, network addresses, authentication method, and the number that the router dials to connect to the central-site router.

		Prompt	Command
Step 1	Create an ISDN dialer interface, and enter configuration mode for the interface. The number that you assign in this command must match the number you assigned with the **backup interface** command when you configured the primary connection to the second central-site router.	`1600(config)#`	`interface Dialer2`
Step 2	Enable IP routing without assigning an IP address.	`1600(config-if)#`	`ip unnumbered ethernet0`
Step 3	Configure this interface for PPP packet encapsulation.	`1600(config-if)#`	`encapsulation ppp`
Step 4	Configure this interface with an IPX network number.	`1600(config-if)#`	`ipx network` *`ABCD`*
Step 5	Configure the name of the central-site router that this interface dials. The name that you enter with this command should be the same name that you entered with the **username password** command in the "Configuring Security" section.	`1600(config-if)#`	`dialer remote-name` *`HQ2`*
Step 6	Configure the number that the interface dials to connect to the central-site router.	`1600(config-if)#`	`dialer string` *`5551122`*
Step 7	Specify that the router can have only one call connected to the first central-site router at any one time.	`1600(config-if)#`	`dialer max-call 1`
Step 8	Assign this interface to a dialer pool.		`dialer pool` *`1`*
Step 9	Assign this interface to a dialer group.	`1600(config-if)#`	`dialer-group` *`1`*
Step 10	Specify that CHAP authentication is performed when this interface connects to the central-site router.	`1600(config-if)#`	`ppp authentication chap`
Step 11	Enable the configuration changes for this interface.	`1600(config-if)#`	`no shutdown`
Step 12	Exit configuration mode for this subinterface.	`1600(config-if)#`	`exit`

Configuring Routing Protocols

Use this table to configure the router for Enhance Interior Gateway Routing Protocol (EIGRP) routing.

		Prompt	Command
Step 1	Configure the router for IP EIGRP routing.	`1600(config) #`	`router eigrp` *`1`*
Step 2	Configure the IP network address for EIGRP routing.	`1600(config-router)#`	`network` *`172.16.0.0`*
Step 3	Exit router configuration mode.	`1600(config-router)#`	`exit`

Configuring Command Line Access to the Router

Use this table to configure some parameters that control access to the router, including the type of terminal line used with the router, how long the router waits for a user entry before it times out, and the password used to start a terminal session with the router.

		Prompt	Command
Step 1	Specify the console terminal line.	`1600(config)#`	**`line console`** *`0`*
Step 2	Set the interval that the EXEC command interpreter waits until user input is detected.	`1600(config-line)#`	**`exec-timeout`** *`5`*
Step 3	Specify a virtual terminal for remote console access	`1600(config-line)#`	**`line vty`** *`0 4`*
Step 4	Specify a password on the line.	`1600(config-line)#`	**`password`** *`lineaccess`*
Step 5	Enable password checking at terminal session login.	`1600(config-line)#`	**`login`**
Step 6	Exit configuration mode.	`1600(config-line)#`	`end`

ISDN as a Backup Connection with Floating Static Routes

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

These are the major tasks when configuring your router:

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

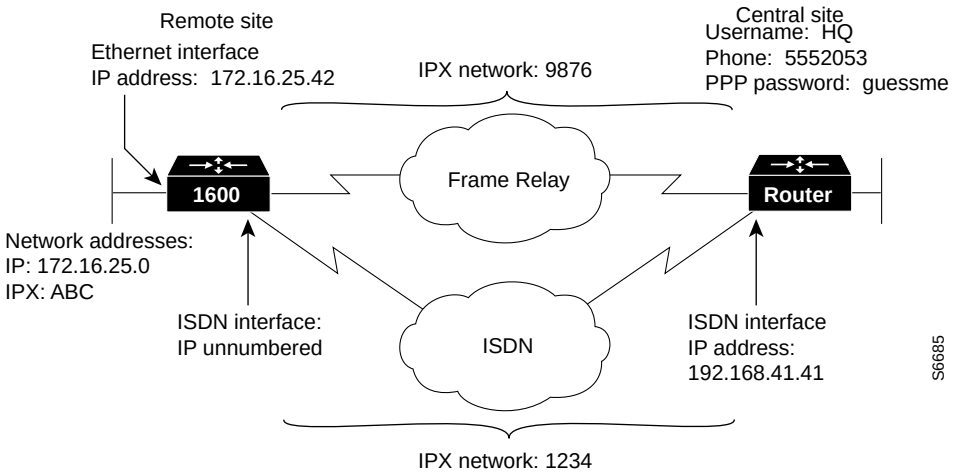
Floating Static Routes

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

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

Figure 5-4 illustrates the example configuration that is used in this section.

Figure 5-4 ISDN as Backup Connection with Floating Static Routes Example Configuration



Assumptions

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

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

Configuring Global Parameters

Use this table to configure the router for some global parameters, including the ISDN switch type that the router is connected to through the ISDN line, and how log and debug messages are timestamped.

		Prompt	Command
Step 1	Enter configuration mode.	`1600#`	`configure terminal`
Step 2	Configure the router to show the date and time of all debug messages. This command is optional, but recommended if you use debug commands to troubleshoot your configuration.	`1600(config)#`	`service timestamps debug datetime msec`
Step 3	Configure the router to show the date and time of all log messages. This command is optional, but recommended if you use the verification steps described in this guide. This feature is enabled for all the example command output shown in this guide.	1600(config)#	service timestamps log datetime msec
Step 4	Configure the type of central office switch being used on the ISDN interface. Use the keyword that matches the ISDN switch type that you are using: • **basic-ts013** —Australian TS013 switches • **basic-1tr6** —German 1TR6 ISDN switches • **basic-nwnet3**—Norway NET3 switches (phase 1) • **basic-net3**—NET3 ISDN switches • **vn2**—French VN2 ISDN switches • **vn3**—French VN3 ISDN switches • **ntt**—Japanese NTT ISDN switches • **basic-5ess**—AT&T basic rate switches • **basic-dms100**—NT DMS-100 basic rate switches • **basic-ni1**—National ISDN-1 switches • **basic-nznet3**—New Zealand Net3 switches	1600(config)#	**isdn switch-type** *basic-ni1*

Configuring Security

Use this table to configure the router with some security measures, the router host name, the password used to prevent unauthorized access to the router, and the username and password that are used for Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) authentication with the central-site router.

		Prompt	Command
Step 1	Configure the router with a host name, which is used in prompts and default configuration file names. For PPP authentication, the host name entered with this command must match the username of the central-site router.	`1600(config)#`	**`hostname`** *`1600`*
Step 2	Specify a password to prevent unauthorized access to the router.	`1600(config)#`	**`enable password`** *`1600user`*
Step 3	Specify the password used during caller identification and CHAP and PAP authentication. For CHAP and PAP authentication, the username entered with this command must match the host name of the central-site router.	`1600(config)#`	**`username`** *`HQ`* **`password`** *`guessme`*

Configuring the Ethernet Interface

Use this table to configure the Ethernet interface (which connects the router to your local network) for IP routing.

		Prompt	Command
Step 1	Enter configuration mode for the Ethernet interface.	`1600(config)#`	`interface Ethernet0`
Step 2	Configure this interface with an IP address and a subnet mask.	`1600(config-if)#`	**`ip address`** *`172.16.25.1 255.255.255.224`*

		Prompt	Command
Step 3	Enable the interface and the configuration changes that you have just made on the interface.	`1600(config-if)#`	`no shutdown`
Step 4	Exit configuration mode for the this interface.	`1600(config-if)#`	`exit`

Configuring the Frame Relay Interface

Use this table to configure parameters for the Frame Relay interface, such as IP routing and a data link connection identifier (DLCI) for the interface.

		Prompt	Command
Step 1	Enter configuration mode for the serial interface	`1600(config)#`	`interface Serial0`
Step 2	Disable IP routing on this interface.	`1600(config-if)#`	`no ip address`
Step 3	Set the encapsulation method on this interface to Frame Relay.	`1600(config-if)#`	`encapsulation frame-relay`
Step 4	Enable the interface and the configuration changes that you have just made on the interface.	`1600(config-if)#`	`no shutdown`
Step 5	Exit configuration mode for this interface.	`1600(config-if)#`	`exit`

Configuring the Frame Relay Subinterface

Use this table to configure the Frame Relay subinterface with IP and IPX network addresses.

		Prompt	Command
Step 1	Enter configuration mode for the serial subinterface and specify this interface as a point-to-point connection.	`1600(config)#`	`interface serial0.1 point-to-point`
Step 2	Configure this subinterface with an IP address.	`1600(config-if)#`	**`ip address`** *`192.168.39.41 255.255.255.0`*

		Prompt	Command
Step 3	Configure this subinterface with an IPX network number.	`1600(config-if)#`	`ipx network 9876`
Step 4	Assign a data link connection identifier (DLCI) to the Frame Relay subinterface. If you are unsure of the DLCI, use the number that you recorded in Step 4 of the previous "Verifying Your Configuration" section.	`1600(config-if)#`	**`frame-relay interface-dlci`** *17*
Step 5	Exit configuration mode for this interface.	1600(config-if)#	exit

Configuring the ISDN Interface

Use this table to configure parameters for the ISDN interface, such as IP unnumbered routing, the telephone number used to connect to the central-site router, and PPP authentication.

		Prompt	Command
Step 1	Enter configuration mode for the ISDN interface.	`1600(config)#`	`interface BRI0`
Step 2	Define the service profile identifier (SPID) number assigned by the ISDN service provider to the B1 channel. This step is required only when the service provider has assigned a SPID to your ISDN line. Not all ISDN lines have SPIDs.	`1600(config)#`	**`isdn spid1`** *555987601*
Step 3	Define the SPID number assigned by the ISDN service provider to the B2 channel. This step is required only when the service provider has assigned a SPID to your ISDN line. Not all ISDN lines have SPIDs.	`1600(config)#`	**`isdn spid2`** *555987602*
Step 4	Enable IP routing on this interface without assigning an IP address.	`1600(config-if)#`	`ip unnumbered Ethernet0`
Step 5	Set the encapsulation method on this interface to PPP.	`1600(config-if)#`	`encapsulation ppp`

		Prompt	Command
Step 6	Configure this interface with an IPX network number.	`1600(config-if)#`	**ipx network** *1234*
Step 7	Configure this interface to exchange routing information while the ISDN line is up. Routing updates do not bring up the ISDN line if it is down.	`1600(config-if)#`	**ipx delay** *200*
Step 8	Disable fast switching and autonomous switching on this interface.	`1600(config-if)#`	`no ip route-cache`
Step 9	Set the router to respond to a local server watchdog packets on behalf of a remote client (called *spoofing*).	`1600(config-if)#`	`ipx watchdog-spoof`
Step 10	Configure the ISDN line to go down after a specified number of seconds with no network traffic.	`1600(config-if)#`	`dialer idle-timeout` *300*
Step 11	Configure the telephone number that this interface dials to reach the central site.	`1600(config-if)#`	**dialer-string** *5552053*
Step 12	Assign this interface to a dialer group.	`1600(config-if)#`	**dialer-group** *1*
Step 13	Disable weighted fair queueing for this interface.	`1600(config-if)#`	`no fair-queue`
Step 14	Enable CHAP and PAP authentication on this interface. CHAP authentication is attempted first. If the central-site router does not support CHAP, PAP is used for authentication.	`1600(config-if)#`	`ppp authentication chap pap callin`
Step 15	Enable multilink PPP on this interface.	`1600(config-if)#`	`ppp multilink`
Step 16	Enable the interface and the configuration changes that you have just made on the interface.	`1600(config-if)#`	`no shutdown`
Step 17	Exit configuration mode for this interface.	`1600(config-if)#`	`exit`

Configuring EIGRP Routing

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

		Prompt	Command
Step 1	Configure the IP EIGRP routing process.	`1600(config)#`	**router eigrp** *202*
Step 2	Specify a list of networks for the EIGRP routing process by entering the IP address of the directly connected network.	`1600(config-router)#`	**network** *172.16.0.0*
Step 3	Specify a list of networks for the EIGRP routing process by entering the IP address of the directly connected network.	`1600(config-router)#`	**network** *192.168.39.0*
Step 4	Specify that the router does not forward packets that are destined for a subnet of a network that has no network default route.	`1600(config-router)#`	`ip classless`
Step 5	Exit router configuration mode.	`1600(config-router)#`	`exit`

Configuring When the Router Dials Out

Use the table to configure access lists and static routes that determine when the ISDN line dials the central-site router.

		Prompt	Command
Step 1	Establish a static IP route to the remote network.	`1600(config)#`	**ip route 0.0.0.0 0.0.0.0** *192.168.41.41 150*
Step 2	Establish a static IP route on the BRI interface to the remote network.	`1600(config)#`	**ip route** *192.168.41.41 255.255.0.0* **BRI0**

		Prompt	Command
Step 3	Define a standard access list based on network variables.	`1600(config)#`	**access-list** *101* **deny ip any** *224.0.0.0 31.255.255.255*
Step 4	Define a standard access list based on network variables.	`1600(config)#`	**access-list** *101* **permit ip any any**
Step 5	Define a standard access list based on network variables.	`1600(config)#`	**access-list** *900* **deny any any all any** *457*
Step 6	Define a standard access list based on network variables.	`1600(config)#`	**access-list** *900* **deny rip any rip any rip**
Step 7	Define a standard access list based on network variables.	`1600(config)#`	**access-list** *900* **deny sap any sap any sap**
Step 8	Define a standard access list based on network variables.	`1600(config)#`	**access-list** *900* **permit any any all any all**
Step 9	Define a floating static IPX route to the central-site network.	`1600(config)#`	**ipx route** *CBA 1234.0000.0c75.c689* **floating-static**
Step 10	Define a floating static IPX route to the central-site network.	`1600(config)#`	**ipx route** *CCB 1234.0000.0c75.c689* **floating-static**
Step 11	Define a floating static IPX route to the central-site network.	`1600(config)#`	**ipx route** *5E11 1234.0000.0c75.c689* **floating-static**
Step 12	Define a static route to an IPX server on the central-site network.	`1600(config)#`	**ipx sap** *4 MRKT_SERV 5E11.0000.0000.0001 452 2*
Step 13	Define a static route to an IPX server on the central-site network.	`1600(config)#`	**ipx sap** *4 ENG_SERV CCB.0000.0000.0001 452 2*
Step 14	Define a static route to an IPX server on the central-site network.	`1600(config)#`	**ipx sap** *4 COPR_SERV CBA.0000.0000.0001 452 2*

		Prompt	Command
Step 15	Specify an dialer list by list number and protocol (IPX) to define the "interesting" packets that can trigger a call to the destination.	`1600(config)#`	**dialer-list** *1* **protocol ipx list** *900*
Step 16	Specify an dialer list by list number and protocol (IP) to define the "interesting" packets that can trigger a call to the destination.	`1600(config)#`	**dialer-list** *1* **protocol ip list** *101*

Configuring Command Line Access to the Router

Use this table to configure some parameters that control access to the router, including the type of terminal line used with the router, how long the router waits before it times out, and the password used to start a terminal session with the router.

		Prompt	Command
Step 1	Specify the console terminal line.	`1600(config)#`	**line console** *0*
Step 2	Set the interval that the EXEC command interpreter waits until user input is detected.	`1600(config-line)#`	**exec-timeout** *5*
Step 3	Specify a virtual terminal for remote console access	`1600(config-line)#`	**line vty** *0 4*
Step 4	Specify a password on the line.	`1600(config-line)#`	**password** *lineaccess*
Step 5	Enable password checking at terminal session login.	`1600(config-line)#`	**login**
Step 6	Exit configuration mode.	`1600(config-line)#`	`end`

Verifying Your Configuration

Take the following steps to verify that the ISDN line is configured to back up the Frame Relay line:

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

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

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

Troubleshooting Floating Static Route Problems

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

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

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

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

How Frame Relay Works

Frame Relay is a method of packet-switching that is used for communication between user devices (such as routers, bridges, and host machines) and network devices (such as switching nodes and modems). User devices are called data terminal equipment (DTE) and network devices are called data circuit-terminating equipment (DCE).

Frame Relay services can be provided by either a public network or a network of privately owned equipment serving a single enterprise.

Frame Relay is a streamlined, efficient, high-performance protocol. It is extremely fast because

- It multiplexes many logical data conversations (or virtual circuits) over one physical link. Multiplexing provides flexible and efficient use of bandwidth.
- It uses fiber media/digital transmission links. These types of physical connections have a high level of data integrity, so Frame Relay does not need to perform error checking. Error checking is time-consuming and can decrease WAN performance.
- It does not need to perform flow control procedures because these types of procedures are done by upper-layer protocols. Frame Relay uses a simple congestion notification mechanism to inform user devices when the network become congested. Congestion notification alerts the higher-layer protocols that flow control is needed.

Current Frame Relay standards support permanent virtual circuits (PVCs) that are configured and managed in a Frame Relay network. Cisco IOS software releases 11.2 and later support switched virtual circuits (SVCs) for DTE interfaces.

Frame Relay also has LMI extensions for supporting large, complex internetworks. Any LMI extension known as *common* should be implemented by anyone who supports the LMI specification. Other LMI extensions are known as *optional*.

The different LMI extensions are

- Virtual circuit status messages (common)—Provide communication and synchronization between the network and the user device, periodically report the existence of new PVCs and the deletion of existing PVCs, and provide information about PVC integrity.

- Multicasting (optional)—Allows a sender to transmit a single frame to multiple recipients, supporting the efficient routing of protocol messages and address resolution procedures that typically must be sent to many destinations simultaneously.
- Global addressing (optional)—Gives connection identifiers global rather than local significance, allowing them to be used to identify a specific interface to the Frame Relay network. Global addressing makes the Frame Relay network resemble a local-area network (LAN) in terms of addressing.

How Dialer Profiles Work

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

A *dialer profile* consists of the following elements:

- A *dialer interface* (a logical entity) configuration with one or more dial strings, each used to reach a specific destination subnetwork.
- A *dialer map class* defines all the characteristics for any call to the specified dial string (telephone number).
- An *dialer pool* of physical interfaces to be used by the dialer interface. The physical interfaces in a dialer pool are ordered according to priority.

How Dialer Interfaces Work

A dialer interface configuration is a group of settings the routers uses to connect to a remote network. One dialer interface can use multiple dial strings (telephone numbers). Each dial string is associated with its own dialer map class. The dialer map class defines all the characteristics for any call to the specified dial string. For example, the dialer map class for one destination might specify a 56-kbps ISDN speed and the map class for a different destination might specify a 64-kbps ISDN speed.

How Dialer Pools Work

Each dialer interface uses one group of physical interfaces called a dialer pool. The physical interfaces in a dialer pool are ordered based on priority. One physical interface can belong to multiple dialer pools. ISDN BRI interfaces can set a limit on the minimum and maximum number of B channels reserved by any dialer pools. A channel reserved by a dialer pool remains idle until traffic is directed to the pool.

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