

# Configuring ISDN

---

This chapter describes how to configure a Cisco 1700 router to dial into a central-site router over an Integrated Services Digital Network (ISDN) line and provides verification steps and troubleshooting tips.

This chapter contains the following sections:

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

## Before You Begin

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

- Your Cisco 1700 router hardware is correctly installed according to the *Cisco 1700 Router Hardware Installation Guide* that came with the router.
- Your Cisco 1700 router is using multilink Point-to-Point Protocol (PPP).
- Your ISDN line is installed and correctly configured. See the “Configuring the ISDN Line” chapter in the *Cisco 1700 Router Hardware Installation Guide* for more information on ordering and configuring your ISDN line.

Before you begin configuration, be aware of the following:

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

---

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

---

## Dial-Up ISDN Connection to a Central-Site Router

This section describes how to configure your Cisco 1700 router for IPX when dialing out over an ISDN line. You should configure your router for IP if you want to use Internet services, such as the World Wide Web, or if the network that you are dialing into uses IP. You should configure IPX if your network uses IPX network services, such as NetWare file servers or print servers.

This configuration assumes that the Cisco 1700 router is dialing into a central-site router.

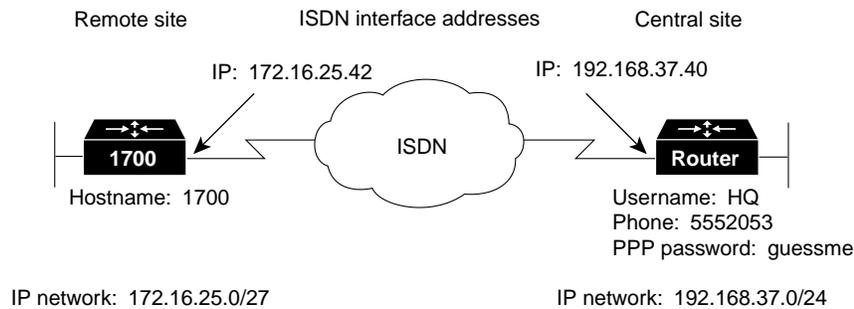
If you are using IP but not IPX on your network, do not enter the commands that include the **ipx** keyword.

These are the major tasks when configuring your router:

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

Figure 3-1 illustrates the example configuration used in this section.

**Figure 3-1 ISDN Example Configuration—Dial-Up to Central Site Router**



14316

## Configuring Global Parameters

Use this table to configure the router for some global parameters.

Step	Task	Router Prompt	Command
1	Enter configuration mode.	Router#	<b>configure terminal</b>
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)#	<b>service timestamps debug datetime msec</b>
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)#	<b>service timestamps log datetime msec</b>
4	Configure the type of central office switch used on the ISDN interface. Use the keyword that matches the ISDN switch type that you are using: <ul style="list-style-type: none"> <li>• <b>basic-ts013</b>—Australian TS013 switches</li> <li>• <b>basic-1tr6</b>—German 1TR6 ISDN switches</li> <li>• <b>basic-nwnet3</b>—Norway NET3 switches (phase 1)</li> <li>• <b>basic-net3</b>—NET3 ISDN switches</li> <li>• <b>vn2</b>—French VN2 ISDN switches</li> <li>• <b>vn3</b>—French VN3 ISDN switches</li> <li>• <b>ntt</b>—Japanese NTT ISDN switches</li> <li>• <b>basic-5ess</b>—Basic rate 5ESS switches</li> <li>• <b>basic-dms100</b>—NT DMS-100 basic rate switches</li> <li>• <b>basic-ni</b>—National ISDN-1 switches</li> <li>• <b>basic-nznet3</b>—New Zealand Net3 switches</li> </ul>	Router(config)#	<b>isdn switch-type basic-ni</b>
5	(Optional) Enable IPX routing and configure the router with an IPX address.	Router(config)#	<b>ipx routing 0060.834f.66dd</b>

## Configuring Security

Use this table to configure the router with some security measures.

Step	Task	Router Prompt	Command
1	Specify a password to prevent unauthorized access to the router.	Router(config)#	<b>enable password</b> <1700user>
2	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)#	<b>hostname</b> 1700
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.	1700(config)#	<b>username</b> HQ <b>password</b> <guessme>

## Configuring the Fast Ethernet Interface

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

Step	Task	Router Prompt	Command
1	Enter configuration mode for the Fast Ethernet interface.	1700(config)#	<b>interface fastethernet0</b>
2	Configure this interface with an IP address and a subnet mask.	1700(config-if)#	<b>ip address</b> 172.16.25.42 255.255.255.224
3	(Optional) Enable IPX routing on this interface and assign the interface with an IPX network address.	1700(config-if)#	<b>ipx network</b> ABC
4	Enable the interface and the configuration changes you have just made on the interface.	1700(config-if)#	<b>no shutdown</b>
5	Exit configuration mode for this interface.	1700(config-if)#	<b>exit</b>

## Verifying Your Configuration

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

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

```
1700# show arp
```

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

```
Protocol Address      Age (min)  Hardware Addr  Type   Interface
Internet 171.16.25.42      -          0060.834f.66dd  ARPA   Fast Ethernet0
1700#
```

**Step 3** The IP address (shown in bold in the example) should be your router Fast Ethernet IP address. If it is not, then re-enter the IP address with **ip address** interface command.

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

## Configuring the ISDN Interface

Use this table to configure the ISDN interface, which connects the router to the central-site router over the wide-area network.

Step	Task	Router Prompt	Command
1	Enter configuration mode for the ISDN interface.	1700(config)#	<b>interface BRI0</b>
2	Add a description of this interface to help you remember what is attached to it.	1700(config-if)#	<b>description</b> <i>ISDN connectivity</i>
3	Enter the service profile identifier (SPID) number assigned by the ISDN service provider to the B1 channel.  This step is required only when the service provider has assigned a SPID to your ISDN line. Not all ISDN lines have SPIDs.	1700(config)#	<b>isdn spid1</b> <i>555987601</i>
4	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.	1700(config)#	<b>isdn spid2</b> <i>555987602</i>
5	Enable IP routing on this interface without assigning an IP address.	1700(config-if)#	<b>ip unnumbered fastethernet0</b>
6	Configure this interface to place a call to multiple sites and to authenticate calls from multiple sites based on IP address and dialer string (phone number).  The name you enter after the <b>name</b> keyword in this command must match the name entered with the <b>username</b> command in the previous “Configuring Security” section.	1700(config-if)#	<b>dialer map ip</b> <i>192.168.37.40 name HQ 5552053</i>
7	(Optional) Enable IPX routing on this interface and assign an IPX network address to the interface.	1700(config-if)#	<b>ipx network</b> <i>123</i>
8	(Optional) Disable IPX fast switching on this interface.	1700(config-if)#	<b>no ipx route-cache</b>
9	(Optional) Set the router to respond to local server watchdog packets on behalf of a remote client (called <i>spoofing</i> ).	1700(config-if)#	<b>ipx watchdog-spoof</b>
10	(Optional) Configure this interface to call multiple sites based on IPX address and dialer string (phone number).	1700(config-if)#	<b>dialer map ipx</b> <i>123.0000.0003.eccb name HQ broadcast 5552053</i>
11	Configure bandwidth on demand by setting the maximum load before the router places another call to a destination.	1700(config-if)#	<b>dialer load-threshold</b> <i>70</i>
12	Assign the dialer interface to a dialer group.	1700(config-if)#	<b>dialer-group</b> <i>1</i>
13	Disable weighted fair queuing on this interface.	1700(config-if)#	<b>no fair-queue</b>

## Dial-Up ISDN Connection to a Central-Site Router

---

14	Configure this interface for PPP encapsulation.	1700(config-if)#	<b>encapsulation ppp</b>
15	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.	1700(config-if)#	<b>ppp authentication chap pap</b>
16	Enable multilink PPP on this interface.	1700(config-if)#	<b>ppp multilink</b>
17	Enable the interface and the configuration changes you have just made on the interface.	1700(config-if)#	<b>no shutdown</b>
18	Exit configuration mode for this interface.	1700(config-if)#	<b>exit</b>

### Verifying Your Configuration

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

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

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

```
1700# show isdn status
The current ISDN Switchtype = basic-5ess
ISDN BRI0 interface
  Layer 1 Status:
    ACTIVE
  Layer 2 Status:
    TEI = 80, State = MULTIPLE_FRAME_ESTABLISHED
  Layer 3 Status:
    No Active Layer 3 Call(s)
  Activated dsl 0 CCBs = 0
  Total Allocated ISDN CCBs =
```

**Step 3** Confirm that the current ISDN switch type (shown in bold in the example) matches the actual switch type that you are using.

**Step 4** Confirm that the “Layer 1 status: ACTIVE” message (shown in bold in the example) appears in the command output.

**Step 5** Confirm that the “State = MULTIPLE\_FRAME\_ESTABLISHED” message (shown in bold in the example) appears in the command output.

---

**Note** In some cases, you might see a “State = TEI\_ASSIGNED” message instead of the “State = MULTIPLE\_FRAME\_ESTABLISHED” message. This message also means that the ISDN line is correctly configured.

---

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

Tips

If you are having problems, do the following:

- Make sure that you entered the **no shutdown** command for the ISDN interface while in interface configuration mode. This enables the configuration changes that you made on the interface.
- Make sure that any external NT1 is functioning correctly. Refer to the documentation that came with the NT1.
- Make sure the ISDN line is correctly configured by checking with the ISDN service provider.

## Configuring Static Routes and Dialing Behavior

Use this table to configure some parameters that control how and when the router dials the central-site router.

Step	Task	Router Prompt	Command
1	Establish a static IP route to the remote network.	1700(config)#	<b>ip route</b> 0.0.0.0 0.0.0.0 192.168.37.40
2	Establish a static IP route to the central-site router through this interface.	1700(config)#	<b>ip route</b> 192.168.37.40 255.255.255.255 <b>BRI0</b>
3	Define a standard access list based on Internet Control Message Protocol (ICMP) traffic.	1700(config)#	<b>access-list</b> 101 permit icmp any any
4	Define a standard access list based on IP traffic.	1700(config)#	<b>access-list</b> 101 permit ip any any
5	Specify an dialer list by list number and protocol (IP) to define the “interesting” packets that can trigger a call to the destination.	1700(config)#	<b>dialer-list</b> 1 protocol ip list 101
6	(Optional) Define a standard access list based on IPX network variables.	1700(config)#	<b>access-list</b> 900 deny any any all any 457
7	(Optional) Define a standard access list based on IPX network variables.	1700(config)#	<b>access-list</b> 900 deny rip any rip any rip
8	(Optional) Define a standard access list based on IPX network variables.	1700(config)#	<b>access-list</b> deny sap and sap any sap
9	(Optional) Define a standard access list based on IPX network variables.	1700(config)#	<b>access-list</b> 900 permit any any all any all
10	(Optional) Specify and access list by list number and protocol (IPX) to define the packets that will trigger the router to make a call to the destination.	1700(config)#	<b>dialer-list</b> 1 protocol ipx list 900

### Verifying Your Configuration

You can verify your configuration to this point by:

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

### Confirming the Static IP Route

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

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

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

**Step 2** Confirm that the “directly connected via BRI” message (shown in bold in the example) appears in the command output:

```
1700# show ip route 192.168.37.40
Routing entry for 192.168.37.40/32
  Known via "connected", distance 0, metric 0 (connected)
  Routing Descriptor Blocks:
  * directly connected, via BRI0
    Route metric is 0, traffic share count is 1
```

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

### Confirming the IPX Route

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

```
1700# show ipx route 123
Codes: C - Connected primary network, c - Connected secondary network
       S - Static, F - Floating static, L - Local (internal), W - IPXWAN
       R - RIP, E - EIGRP, N - NLSP, X - External, A - Aggregate
       s - seconds, u - uses

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

No default route known.

C      123 (PPP),          BR0
```

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

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

### Confirming Connectivity to the Central-Site Router

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

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

```
1700# 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
1700#
*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 data to the central-site router.

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

### Confirming Multilink PPP Configuration for the B1 Channel

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

Take the following steps to perform the first verification step:

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

```
1700# ping 192.168.37.40
```

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

- Step 3** Confirm that the “Master link is Virtual-Access1” message (shown in bold in the example) appears in the command output.

```
1700# show ppp multilink
Bundle HQ, 1 member, Master link is Virtual-Access1
Dialer Interface is BRI0
  0 lost fragments, 0 reordered, 0 unassigned, sequence 0x0/0x0 rcvd/sent
  0 discarded, 0 lost received, 1/255 load
Member Link: 1
BRI0:1
```

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

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

- Step 5** To continue configuration, re-enter global configuration mode.

Take the following steps to perform the second verification step:

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

```
1700# ping 192.168.37.40
```

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

- Step 3** Confirm that the “Open: IPCP” message (shown in bold in the example) appears in the command output:

```
1700# show interface virtual-access 1

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

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

### Confirming Multilink PPP Configuration for the B2 Channel

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

```
1700# ping 192.168.37.40
```

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

---

**Note** One way to perform Step 2 is by reducing the amount of data required to cause the second B channel to dial. Reduce the amount (called the threshold) with the **dialer load-threshold** command, which is described on page 5 in Step 11.

---

**Step 3** Check the LEDs labeled B1 and B2.

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

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

### Tips

If you are having problems, do the following:

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

## Configuring Command-Line Access to the Router

Use this table to configure some parameters that control access to the router.

Step	Task	Router Prompt	Command
1	Specify the console terminal line.	1700(config)#	<b>line console 0</b>
2	Set the interval that the EXEC command interpreter waits until user input is detected.	1700(config-line)#	<b>exec-timeout 5</b>
3	Specify a virtual terminal for remote console access.	1700(config-line)#	<b>line vty 0 4</b>
4	Specify a password on the line.	1700(config-line)#	<b>password &lt;lineaccess&gt;</b>
5	Enable password checking at terminal session login.	1700(config-line)#	<b>login</b>
6	Exit configuration mode.	1700(config-line)#	<b>end</b>

## Troubleshooting

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 routing. Follow these commands with the **ping** command to begin debug output:

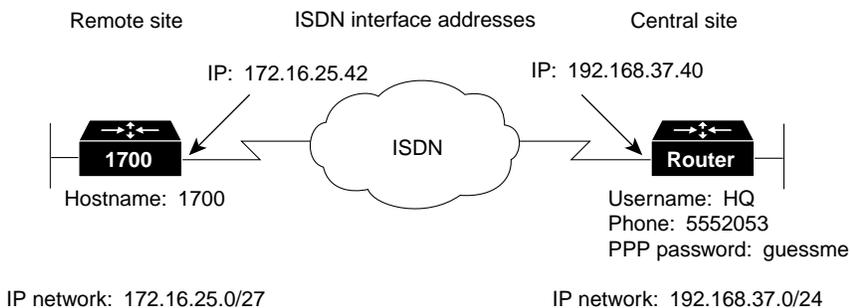
- **debug dialer events**
- **debug isdn events**
- **debug isdn q931**
- **debug isdn q921**
- **debug ppp negotiation**
- **debug ppp authentication**
- **debug ppp multilink events**

## Dial-Up ISDN Connection with Dialer Profiles

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

Figure 3-2 illustrates the example configuration used in this section.

**Figure 3-2 ISDN Example Configuration—Dial-Up with Dialer Profiles**



14316

These are the major tasks when configuring your router:

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

## Configuring Global Parameters

Use this table to configure the router for some global parameters.

Step	Task	Router Prompt	Command
1	Enter configuration mode.	Router#	<b>configure terminal</b>
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)#	<b>service timestamps debug datetime msec</b>
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)#	<b>service timestamps log datetime msec</b>
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: <ul style="list-style-type: none"> <li>• <b>basic-ts013</b>—Australian TS013 switches</li> <li>• <b>basic-1tr6</b>—German 1TR6 ISDN switches</li> <li>• <b>basic-nwnet3</b>—Norway NET3 switches (phase 1)</li> <li>• <b>basic-net3</b>—NET3 ISDN switches</li> <li>• <b>vn2</b>—French VN2 ISDN switches</li> <li>• <b>vn3</b>—French VN3 ISDN switches</li> <li>• <b>ntt</b>—Japanese NTT ISDN switches</li> <li>• <b>basic-5ess</b>—Basic rate 5ESS switches</li> <li>• <b>basic-dms100</b>—NT DMS-100 basic rate switches</li> <li>• <b>basic-ni</b>—National ISDN-1 switches</li> <li>• <b>basic-nznet3</b>—New Zealand Net3 switches</li> </ul>	Router(config)#	<b>isdn switch-type basic-ni</b>

## Verifying Your Configuration

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

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

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

```
1700# show isdn status
The current ISDN Switchtype = basic-5ess
ISDN BRI0 interface
  Layer 1 Status:
    ACTIVE
  Layer 2 Status:
    TEI = 80, State = MULTIPLE_FRAME_ESTABLISHED
  Layer 3 Status:
    No Active Layer 3 Call(s)
    Activated dsl 0 CCBS = 0
    Total Allocated ISDN CCBS =
```

**Step 3** Confirm that the current ISDN switch type (shown in bold in the example) matches the actual switch type that you are using.

**Step 4** Confirm that the following messages (shown

**Step 5** Confirm that the “Layer 1 status: ACTIVE” message (shown in bold in the example) appears in the command output.

**Step 6** Confirm that the “State = MULTIPLE\_FRAME\_ESTABLISHED” message (shown in bold in the example) appears in the command output.

---

**Note** In some cases, you might see a “State = TEI\_ASSIGNED” message instead of the “State = MULTIPLE\_FRAME\_ESTABLISHED” message. This message also means that the ISDN line is correctly configured.

---

**Step 7** To continue configuration, re-enter global configuration mode.

## Tips

If you are having problems, do the following:

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

## Configuring Security

Use this table to configure the router with security measures.

Step	Task	Router Prompt	Command
1	Configure the router with a host name, which is used in prompts and default configuration file names.  For PPP authentication, the hostname entered with this command must match the username of the central-site router.	Router(config)#	<b>hostname</b> 1700
2	Specify a password to prevent unauthorized access to the router.	1700(config)#	<b>enable password</b> <1700user>
3	Specify the password that will be used during CHAP caller identification and PAP.  For PPP authentication, the username entered with this command must match the hostname of the central-site router.	1700(config)#	<b>username</b> HQ <b>password</b> <guessme>

## Configuring the Fast Ethernet Interface

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

Step	Task	Router Prompt	Command
1	Enter configuration mode for the Fast Ethernet interface.	1700(config)#	<b>interface fastethernet0</b>
2	Configure this interface with an IP address and a subnet mask.	1700(config-if)#	<b>ip address</b> 172.16.25.42 255.255.255.224
3	Enable IPX routing on this interface.	1700(config-if)#	<b>ipx network</b> ABC
4	Enable the interface and the configuration changes you have just made on the interface.	1700(config-if)#	<b>no shutdown</b>
5	Exit configuration mode for this interface.	1700(config-if)#	<b>exit</b>

## Configuring the ISDN Interface

Use this table to configure the ISDN interface, which connects the router to the central-site router over the wide-area network.

Step	Task	Router Prompt	Command
1	Enter configuration mode for the ISDN interface.	1700(config)#	<b>interface BRI0</b>
2	Add a description of the ISDN interface to help you remember what is attached to it.	1700(config-if)#	<b>description</b> ISDN connectivity
3	Enter the service profile identifier (SPID) number that has been assigned by the ISDN service provider for the B1 channel.  This step is required only when the service provider has assigned a SPID to your ISDN line. Not all ISDN lines required SPIDs.	1700(config)#	<b>isdn spid1</b> 555987601

4	Define the SPID number that has been assigned by the ISDN service provider for the B2 channel.  This step is required only when the service provider has assigned a SPID to your ISDN line. Not all ISDN lines required SPIDs.	1700(config)#	<b>isdn spid2 555987602</b>
5	Disable IP routing on this interface.	1700(config-if)#	<b>no ip address</b>
6	Put this interface in a dialing pool.  As an option, you can also assign a priority to the interface with this command.	1700(config-if)#	<b>dialer pool-member 1</b>
7	Set the encapsulation method on this interface to PPP.	1700(config-if)#	<b>encapsulation ppp</b>
8	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.	1700(config-if)#	<b>ppp authentication chap pap</b>
9	Enable multilink PPP on this interface.	1700(config-if)#	<b>ppp multilink</b>
10	Enable the interface and the configuration changes you have just made on the interface.	1700(config-if)#	<b>no shutdown</b>
11	Exit configuration mode for this interface.	1700(config-if)#	<b>exit</b>

## Configuring the Dialer Interface

Use this table to create a dialer interface and configure it for Dial-on-Demand Routing (DDR).

Step	Task	Router Prompt	Command
1	Create a dialer interface.	1700(config)#	<b>interface Dialer10</b>
2	Enable IP routing on this interface without assigning an IP address.	1700(config-if)#	<b>ip unnumbered fastethernet0</b>
3	Enable IPX routing on this interface.	1700(config-if)#	<b>ipx network 123</b>
4	Disable IPX fast switching on this interface.	1700(config-if)#	<b>no ipx route-cache</b>
5	Set the router to respond to a local server watchdog packets on behalf of a remote client (called <i>spoofing</i> ).	1700(config-if)#	<b>ipx watchdog-spoof</b>
6	Specify the central-site router CHAP authentication name.	1700(config-if)#	<b>dialer remote-name HQ</b>
7	Specify the string (telephone number) to be called for this interface when calling a single site.	1700(config-if)#	<b>dialer string 5552053</b>
8	Put this interface in a dialing pool.  As an option, you can also assign a priority to the interface with this command.	1700(config-if)#	<b>dialer pool 1</b>
9	Assign the dialer interface to a dialer group.	1700(config-if)#	<b>dialer-group 1</b>
10	Set the encapsulation method on this interface to PPP.	1700(config-if)#	<b>encapsulation ppp</b>
11	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.	1700(config-if)#	<b>ppp authentication chap pap</b>

12	Enable multilink PPP on this interface.	1700(config-if)#	<b>ppp multilink</b>
13	Enable the interface and the configuration changes you have just made on the interface.	1700(config-if)#	<b>no shutdown</b>
14	Exit configuration mode for this interface.	1700(config-if)	<b>exit</b>

### Verifying Your Configuration

You can verify your configuration to this point by:

- Confirming Multilink PPP Configuration for the B1 Channel
- Confirming Multilink PPP Configuration for the B1 Channel

#### Confirming Multilink PPP Configuration for the B1 Channel

- Step 1** Confirm that the ISDN is up and connected to the central-site router.
- Step 2** From the privileged EXEC command mode, enter the **show ppp multilink** command.
- Step 3** Confirm that the “Master link is Virtual-Access1” message (shown in bold in the example) appears in the command output.

```
1700# show ppp multilink
Bundle HQ, 1 member, Master link is Virtual-Access1
Dialer Interface is BRI0
  0 lost fragments, 0 reordered, 0 unassigned, sequence 0x0/0x0 rcvd/sent
  0 discarded, 0 lost received, 1/255 load
Member Link: 1
BRI0:1
```

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

#### Confirming Multilink PPP Configuration for the B1 Channel

- Step 1** Confirm that the ISDN is up and connected to the central-site router.
- Step 2** From the privileged EXEC command mode, enter the **show interface** command.
- Step 3** Confirm that the “LCP Open, multilink Open” message (shown in bold in the example) appears in the command output:

```
1700# show interface bri 0 1 2
BRI0:1 is up, line protocol is up
Hardware is BRI with U interface and external S bus interface
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 3/255
Encapsulation PPP, loopback not set, keepalive set (10 sec)
LCP Open, multilink Open
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo...
```

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

## Configuring When the Router Dials Out

Use this table to configure some parameters that control how and when the router dials the central-site router, such as access lists and dialer lists.

Step	Task	Router Prompt	Command
1	Establish a static IP route to the remote network.	1700(config)#	<b>ip route</b> 192.168.37.0 255.255.255.0 192.168.37.40
2	Establish a static IP route to the remote network through the router BRI interface.	1700(config)#	<b>ip route</b> 192.168.37.40 255.255.255.255 BRI0
3	Define a standard access list based on your network.	1700(config)#	<b>access-list</b> 101 permit icmp any any
4	Define a standard access list based on your network.	1700(config)#	<b>access-list</b> 101 deny ip any any
5	Define a standard access list based on your network.	1700(config)#	<b>access-list</b> 900 deny any any all any 457
6	Define a standard access list based on your network.	1700(config)#	<b>access-list</b> 900 deny rip any rip any rip
7	Define a standard access list based on your network.	1700(config)#	<b>access-list</b> 900 deny sap any sap any sap
8	Define a standard access list based on your network.	1700(config)#	<b>access-list</b> 900 permit any any all any all
9	Specify an access list by list number and protocol (IP) to define the “interesting” packets that can trigger a call to the destination.	1700(config)#	<b>dialer-list 1 protocol ip list 101</b>
10	Specify an access list by list number and protocol (IPX) to define the “interesting” packets that can trigger a call to the destination.	1700(config)#	<b>dialer-list 1 protocol ipx list 900</b>

### Verifying Your Configuration

You can verify your configuration to this point by:

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

#### Confirming the IP Static Route

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

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

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

**Step 2** Confirm that the “directly connected via BRI” message (shown in bold in the following example) appears in the command output:

```
1700# show ip route 192.168.37.40
Routing entry for 192.168.37.40/32
  Known via "connected", distance 0, metric 0 (connected)
  Routing Descriptor Blocks:
    * directly connected, via BRI0
```

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

### Confirming Connectivity to the Central-Site Router

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

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

**Step 2** Wait for the “ISDN-6-CONNECT” message (shown in bold in the example):

```
1700# 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
1700#
*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 3** Enter the **ping** command followed by the IP address of the central-site router again:

```
1700# ping 192.168.37.40

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.37.40, timeout is 2 seconds:
.!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/43/48 ms
1700#
*Mar 1 03:37:46.526: %LINK-3-UPDOWN: Interface BRI0:1, changed state to up
*Mar 1 03:37:46.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:1, changed state to up
*Mar 1 03:37:46.939: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
*Mar 1 03:37:47.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up
*Mar 1 03:35:57.217: %ISDN-6-CONNECT: Interface BRI0:1 is now connected to 5552053 HQ
```

**Step 4** If the success rate (shown in bold in the example) is 100 percent, this verification step is successful. If the success

**Step 5** To continue configuration, re-enter global configuration mode.

### Tips

If you are having problems, do the following:

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

## Configuring Command-Line Access to the Router

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

Step	Task	Router Prompt	Command
1	Specify the console terminal line.	1700(config)#	<b>line console 0</b>
2	Set the interval that the EXEC command interpreter waits until user input is detected.	1700(config-line)#	<b>exec-timeout 5</b>

3	Specify a virtual terminal for remote console access	1700(config-line)#	<b>line vty 0 4</b>
4	Specify a password on the line.	1700(config-line)#	<b>password &lt;lineaccess&gt;</b>
5	Enable password checking at terminal session login.	1700(config-line)#	<b>login</b>
6	Exit configuration mode.	1700(config-line)#	<b>end</b>

## Troubleshooting Dialer Profile Problems

If you are having problems, or the output that you received during the verification steps is very different than 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 dialer profiles with ISDN. Most of these commands require that you follow with the **ping** command to begin debug output:

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

## Leased Line ISDN Connection to a Central-Site Router

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

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

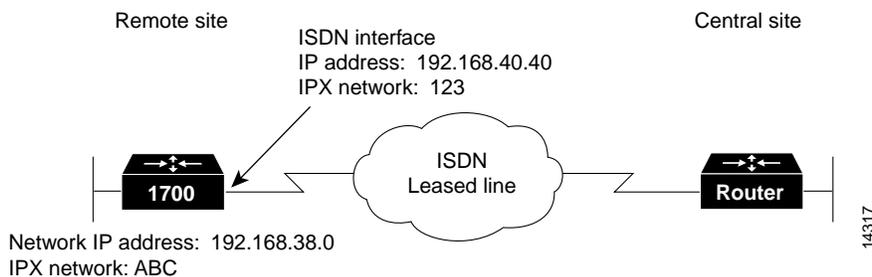
These are major tasks when configuring your router for a leased line ISDN connection:

- Configuring Global Parameters
- Configuring Security
- Configuring IPX Routing
- Configuring the ISDN Line for Leased Line

- Configuring the ISDN Interface
- Configuring the ISDN Subinterfaces
- Configuring Command-Line Access to the Router

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

**Figure 3-3 ISDN Leased Line Example Configuration**



## Configuring Global Parameters

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

Step	Task	Router Prompt	Command
1	Enter configuration mode.	Router#	<b>configure terminal</b>
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)#	<b>service timestamps debug datetime msec</b>
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)#	<b>service timestamps log datetime msec</b>

Step	Task	Router Prompt	Command
4	<p>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:</p> <ul style="list-style-type: none"> <li>• <b>basic-ts013</b>—Australian TS013 switches</li> <li>• <b>basic-1tr6</b>—German 1TR6 ISDN switches</li> <li>• <b>basic-nwnet3</b>—Norway NET3 switches (phase 1)</li> <li>• <b>basic-net3</b>—NET3 ISDN switches</li> <li>• <b>vn2</b>—French VN2 ISDN switches</li> <li>• <b>vn3</b>—French VN3 ISDN switches</li> <li>• <b>ntt</b>—Japanese NTT ISDN switches</li> <li>• <b>basic-5ess</b>—Basic rate 5ESS switches</li> <li>• <b>basic-dms100</b>—NT DMS-100 basic rate switches</li> <li>• <b>basic-ni</b>—National ISDN-1 switches</li> <li>• <b>basic-nznet3</b>—New Zealand Net3 switches</li> </ul>	Router(config)#	<b>isdn switch-type</b> <i>basic-ni</i>

## Configuring Security

Use this table to configure the router with some security measures.

Step	Task	Router Prompt	Command
1	Specify a password to prevent unauthorized access to the router.	Router(config)#	<b>enable password</b> <1700user>
2	<p>Configure the router with a host name, which is used in prompts and default configuration file names.</p> <p>For PPP authentication, the host name entered with this command must match the username of the central-site router.</p>	Router(config)#	<b>hostname</b> 1700
3	<p>Specify the password used during caller identification and CHAP and PAP authentication.</p> <p>For CHAP and PAP authentication, the username entered with this command must match the host name of the central-site router.</p>	1700(config)#	<b>username</b> <i>HQ</i> <b>password</b> <guessme>

## Configuring IPX Routing

Use this table to enable IPX routing on the router. The default setting for the router is IPX routing disabled.

Step	Task	Router Prompt	Command
1	Enable IPX routing and configure the router with an IPX address.	1700(config)#	<b>ipx routing 0060.834f.66dd</b>

## Configuring the ISDN Line for Leased Line

Use this table to set up the ISDN line for a leased line configuration.

Step	Task	Router Prompt	Command
1	Define a virtual template from which this multilink PPP bundle interface can replicate its interface parameters.	1700(config)#	<b>multilink virtual-template 1</b>
2	Configure the BRI interface to use the ISDN physical connection as a leased line service. If you want to combine both B channels into a single data pipe, enter the <b>128</b> keyword with this command.	1700(config)#	<b>isdn leased-line BRI0 128</b>

## Configuring the Fast Ethernet Interface

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

Step	Task	Router Prompt	Command
1	Enter configuration mode for the Fast Ethernet interface.	1700(config)#	<b>interface fastethernet0</b>
2	Configure this interface with an IP address and a subnet mask.	1700(config-if)#	<b>ip address 192.168.38.42 255.255.255.0</b>
3	Configure this interface with an IPX network address.	1700(config-if)#	<b>ipx network ABC</b>
4	Associate the virtual template with this interface.	1700(config-if)#	<b>interface Virtual-Template1</b>
5	Configure the virtual template interface with an IP address and a subnet mask.	1700(config-if)#	<b>ip address 192.168.40.40 255.255.255.0</b>
6	Configure the virtual template interface with an IPX network address.	1700(config-if)#	<b>ipx network 123</b>
7	Set the encapsulation method on this interface to PPP.	1700(config-if)#	<b>encapsulation ppp</b>
8	Enable multilink PPP on this interface.	1700(config-if)#	<b>ppp multilink</b>
9	Enable the interface and the configuration changes you have just made on the interface.	1700(config-if)#	<b>no shutdown</b>
10	Exit configuration mode for this interface.	1700(config-if)#	<b>exit</b>

## Configuring the ISDN Interface

Use this table to clear the IP address from the ISDN interface.

Step	Task	Router Prompt	Command
1	Enter configuration mode for the BRI interface.	1700(config)#	<b>interface BRI0</b>
2	Disable IP routing on the BRI0 interface.	1700(config-if)#	<b>no ip address</b>
3	Exit configuration mode for this interface.	1700(config-if)#	<b>exit</b>

## Configuring the ISDN Subinterfaces

Use this table to create and configure two ISDN subinterfaces, which connect your router to the central-site router over the wide-area network.

Step	Task	Router Prompt	Command
1	Enter configuration mode for the BRI0:1 subinterface	1700(config-if)#	<b>interface BRI0:1</b>
2	Enable IP routing on this interface without assigning an IP address.	1700(config-if)#	<b>ip unnumbered Virtual-Template/</b>
3	Set the encapsulation method on this interface to PPP.	1700(config-if)#	<b>encapsulation ppp</b>
4	Enable multilink PPP on this interface.	1700(config-if)#	<b>ppp multilink</b>
5	Enter configuration mode for the BRI0:2 subinterface.	1700(config-if)#	<b>interface BRI0:2</b>
6	Enable IP routing on this interface without assigning an IP address.	1700(config-if)#	<b>ip unnumbered Virtual-Template/</b>
7	Set the encapsulation method on this interface to PPP.	1700(config-if)#	<b>encapsulation ppp</b>
8	Enable multilink PPP on this interface.	1700(config-if)#	<b>ppp multilink</b>
9	Exit configuration mode for this interface.	1700(config-if)	<b>exit</b>

## Configuring Dynamic IP Routing

Use this table to configure the router for dynamic IP routing.

Step	Task	Router Prompt	Command
1	Configure the router to forward packets addressed to a subnet of a network with no network default route.	1700(config)#	<b>ip classless</b>
2	Specify dynamic routing.	1700(config)#	<b>ip route 0.0.0.0 0.0.0.0 192.168.40.41</b>

### Verifying Your Configuration

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

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

**Step 2** Wait for the “ISDN-6-CONNECT” message (shown in bold in the example):

```
1700# 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
1700#
*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 3** Enter the **ping** command followed by the IP address of the central-site router again:

```
1700# ping 192.168.37.40

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.37.40, timeout is 2 seconds:
.!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/43/48 ms
1700#
*Mar 1 03:37:46.526: %LINK-3-UPDOWN: Interface BRI0:1, changed state to up
*Mar 1 03:37:46.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:1, changed state to up
*Mar 1 03:37:46.939: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
*Mar 1 03:37:47.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up
*Mar 1 03:35:57.217: %ISDN-6-CONNECT: Interface BRI0:1 is now connected to 5552053 HQ
```

**Step 4** If the success rate (shown in bold in the example) is 100 percent, this verification step is successful. If the success

**Step 5** To continue configuration, re-enter global configuration mode.

**Step 6** If the router is not successfully transferring data to the central-site router (if the success rate is less than 60 percent), take the following steps:

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

**Step 7** To continue configuration, re-enter global configuration mode.

## Configuring Command-Line Access to the Router

Use this table to configure some parameters that control access to the router, such as 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.

Step	Task	Router Prompt	Command
1	Specify the console terminal line.	1700(config)#	<b>line console 0</b>
2	Set the interval that the EXEC command interpreter waits until user input is detected.	1700(config-line)#	<b>exec-timeout 5</b>
3	Specify a virtual terminal for remote console access.	1700(config-line)#	<b>line vty 0 4</b>
4	Specify a password on the line.	1700(config-line)#	<b>password &lt;lineaccess&gt;</b>
5	Enable password checking at terminal session login.	1700(config-line)#	<b>login</b>
6	Exit configuration mode.	1700(config-line)#	<b>end</b>

## Troubleshooting Leased Line 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 the **debug** commands that are helpful when troubleshooting an ISDN leased line. Follow these commands with the **ping** command to begin debug output.

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

## Dial-In ISDN BRI Pool

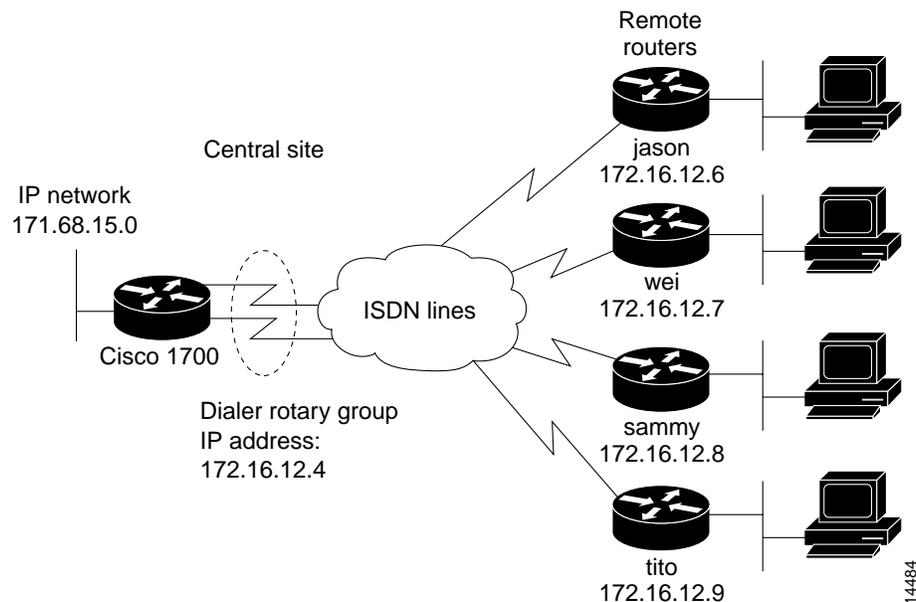
This section describes how to configure a Cisco 1700 router with two ISDN BRI interfaces to function as a dial-in server. In this example, the Cisco 1700 router functions as the central-site router that accepts dial-in connections from remote routers.

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

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

Figure 3-4 illustrates the example configuration used in this chapter.

**Figure 3-4 ISDN Example Configuration—Dial-In ISDN Pool**



## Configuring Global Parameters

Use this table to configure some global router parameters.

Step	Task	Prompt	Command
1	Enter configuration mode.	Router#	<b>configure terminal</b>
2	Configure the router to show the date and time of all debug messages.  This command is optional, but recommended in the event that you use debug commands to troubleshoot your configuration.	Router(config)#	<b>service timestamps debug datetime msec</b>
3	Configure the router to show the date and time of all log messages.  This command is optional, but recommended in the event that 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)#	<b>service timestamps log datetime msec</b>
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:  <ul style="list-style-type: none"> <li>• <b>basic-ts013</b>—Australian TS013 switches</li> <li>• <b>basic-1tr6</b>—German 1TR6 ISDN switches</li> <li>• <b>basic-nwnet3</b>—Norway NET3 switches (phase 1)</li> <li>• <b>basic-net3</b>—NET3 ISDN switches</li> <li>• <b>vn2</b>—French VN2 ISDN switches</li> <li>• <b>vn3</b>—French VN3 ISDN switches</li> <li>• <b>ntt</b>—Japanese NTT ISDN switches</li> <li>• <b>basic-5ess</b>—Basic rate 5ESS switches</li> <li>• <b>basic-dms100</b>—NT DMS-100 basic rate switches</li> <li>• <b>basic-ni</b>—National ISDN-1 switches</li> <li>• <b>basic-nznet3</b>—New Zealand Net3 switches</li> </ul>	1700(config)#	<b>isdn switch-type <i>basic-ni</i></b>

## Configuring Security

Use this table to configure some security measures.

Step	Task	Prompt	Command
1	Specify a password to prevent unauthorized access to the router.	Router(config)#	<b>enable password</b> <1700user>
2	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)#	<b>hostname</b> 1700
3	Specify the password used during caller identification and CHAP and PAP authentication.  For CHAP and PAP authentication, the hostname of every remote router that dials into the Cisco 1700 router must be entered with this command, along with the password used to authenticate that router.	1700(config)#	<b>username</b> jason <b>password</b> <foot> <b>username</b> wei <b>password</b> <letmein> <b>username</b> sammy <b>password</b> <bar> <b>username</b> tito <b>password</b> <knockknock>

## Configuring the Fast Ethernet Interface

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

Step	Task	Prompt	Command
1	Enter configuration mode for this interface.	1700(config)#	<b>interface fastethernet0</b>
2	Configure this interface with an IP address and a subnet mask.	1700(config-if)#	<b>ip address</b> 171.68.15.33 255.255.255.248
3	Enable this interface and the configuration changes that you have just made.	1700(config-if)#	<b>no shutdown</b>
4	Exit configuration mode for this interface.	1700(config-if)#	<b>exit</b>

## Configuring the ISDN Interfaces

Use this table to configure the two ISDN interfaces that accept calls from remote routers.

Step	Task	Prompt	Command
1	Enter configuration mode for the first ISDN interface.	1700(config)#	<b>interface BRI0</b>
2	Remove any IP addresses that might be assigned to this interface.	1700(config-if)#	<b>no ip address</b>
3	Configure the interface for PPP packet encapsulation.	1700(config-if)#	<b>encapsulation ppp</b>
4	Configure this interface to be included in the dialer rotary group that you will configure in the following task table.	1700(config-if)#	<b>dialer rotary-group</b> 100
5	Disable weighted fair queuing on this interface.	1700(config-if)#	<b>no fair queue</b>

Step	Task	Prompt	Command
6	Enable this interface and the configuration changes you have just made.	1700(config-if)#	<b>no shutdown</b>
7	Exit configuration mode for this interface.	1700(config-if)#	<b>exit</b>
8	Enter configuration mode for the second ISDN interface.	1700(config)#	<b>interface BRI1</b>
9	Remove any IP addresses that might be assigned to this interface.	1700(config-if)#	<b>no ip address</b>
10	Configure the interface for PPP packet encapsulation.	1700(config-if)#	<b>encapsulation ppp</b>
11	Configure this interface to be included in the dialer rotary group that you will configure in the following task table.	1700(config-if)#	<b>dialer rotary-group 100</b>
12	Disable weighted fair queueing on this interface.	1700(config-if)#	<b>no fair queue</b>
13	Enable this interface and the configuration changes you have just made.	1700(config-if)#	<b>no shutdown</b>
14	Exit configuration mode for this interface.	1700(config-if)#	<b>exit</b>

## Configuring a Dialer Interface

Use this table to configure the two ISDN interfaces as one dialer interface that accepts calls from remote routers.

Step	Task	Prompt	Command
1	Create a dialer rotary group interface and enter configuration mode for that interface. The number (in this example, 100) is an integer that you select to identify the interface.	1700(config)#	<b>interface dialer 100</b>
2	Configure this interface with an IP address.	1700(config-if)#	<b>ip address 172.16.12.4 255.255.255.240</b>
3	Configure this interface for PPP encapsulation.	1700(config-if)#	<b>encapsulation ppp</b>
4	Specify that dial-on-demand routing (DDR) is supported on this interface.	1700(config-if)#	<b>dialer in-band</b>
5	Configure the ISDN line to go down after a specified number of seconds with no network traffic.	1700(config-if)#	<b>dialer idle-timeout 300</b>
6	Configure this interface to receive and authenticate calls from multiple sites based on IP address and dialer string. You must enter this command for every remote router that will dial into your router.  The name you enter after the <b>name</b> keyword in this command must match the name entered with the <b>username</b> command in the previous “Configure Security” section.	1700(config-if)#	<ul style="list-style-type: none"> <li>• <b>dialer map ip 172.16.12.6 name jason broadcast 5553756</b></li> <li>• <b>dialer map ip 172.16.12.7 name wei broadcast 5553756</b></li> <li>• <b>dialer map ip 172.16.12.8 name sammy broadcast 5553756</b></li> <li>• <b>dialer map ip 172.16.12.9 name tito broadcast 5553756</b></li> </ul>
7	Configure bandwidth on demand by setting the maximum load before the router places another call to a destination.	1700(config-if)#	<b>dialer load-threshold 70</b>
8	Assign the dialer interface to a dialer group.	1700(config-if)#	<b>dialer-group 1</b>
9	Disable weighted fair queueing on this interface.	1700(config-if)#	<b>no fair-queue</b>

## Dial-In ISDN BRI Pool

---

Step	Task	Prompt	Command
10	Enable multilink PPP on this interface.	1700(config-if)#	<b>ppp multilink</b>
11	Enable CHAP or PAP authentication on this interface.	1700(config-if)#	<b>ppp authentication chap</b>
12	Enable the dialer interface and the configuration changes that you have just made.	1700(config-if)#	<b>no shutdown</b>
13	Exit configuration mode for this interface.	1700(config-if)#	<b>exit</b>

## 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.

Step	Task	Router Prompt	Command
1	Configure the IP EIGRP routing process and enter router configuration mode.	1700(config)#	<b>router eigrp 109</b>
2	Specify a list of networks for the EIGRP routing process by entering the IP address of the directly connected network.	1700(config-router)#	<b>network 171.68.0.0</b>
3	Configure the router to distribute IP static routes from one routing domain to another.	1700(config-router)#	<b>redistribute static</b>
4	Exit router configuration mode.	1700(config-router)#	<b>exit</b>

## Configuring IP Static Routes and Dial-In Parameters

Use this table to configure an IP static router and access lists that define what type of network traffic will be accepted by the router.

Step	Task	Router Prompt	Command
1	Configure an IP static route used to route data received from remote routers.	1700(config)#	<b>ip route 171.68.0.0 255.255.255.240 171.68.12.1</b>
2	Define a standard access list based on IP network variables.	1700(config)#	<b>access-list 101 deny ip any host 255.255.255.255</b>
3	Define a standard access list based on IP network variables.	1700(config)#	<b>access-list 101 permit ip any any</b>
4	Specify a dialer list by list number and protocol (IP) to define the “interesting” packets that can trigger a call to the destination.	1700(config)#	<b>dialer-list 1 list 101</b>

## Configuring Command-Line Access to the Router

Use this table to configure some parameters that control access to the router, such as 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.

Step	Task	Router Prompt	Command
1	Specify the console terminal line.	1700(config)#	<b>line console 0</b>
2	Set the interval that the EXEC command interpreter waits until user input is detected.	1700(config-line)#	<b>exec-timeout 5</b>
3	Specify a virtual terminal for remote console access.	1700(config-line)#	<b>line vty 0 4</b>
4	Specify a password on the line.	1700(config-line)#	<b>password &lt;lineaccess&gt;</b>
5	Enable password checking at terminal session login.	1700(config-line)#	<b>login</b>
6	Exit configuration mode.	1700(config-line)#	<b>end</b>

