8

Configuring Demand Routing for Primary ISDN Modules

Contents

Overview of ISDN Connections

Integrated Services Digital Network (ISDN) connections are point-to-point dial-up connections that can handle both voice and data over a single line. ISDN provides WAN connections at a lower cost than dedicated WAN connections such as E1- or T1-carrier lines. Like telephone calls, ISDN connections incur costs only when the connection is established.

To establish and maintain the connection through the public carrier network, ISDN connections are divided into two types of channels:

- bearer (B)
- data (D)

B channels carry voice and data over the connection and transmit data at 56 or 64 Kbps. The D channel maintains the connection and transmits the signaling and call-control information at 16 or 64 Kbps.

Two types of ISDN connections are available:

- ISDN Basic Rate Interface (BRI)
- ISDN Primary Rate Interface (PRI)

ISDN BRI provides two 64-Kbps B channels and one 16 Kbps D channel. If you bond or multilink the two B channels in a ISDN BRI connection, the total transmission rate is 128 Kbps. (Multilinking the two channels is discussed in more detail later in this chapter.)

PRI ISDN, on the other hand, provides 23 B channels and 1 D channel in North America and Japan and 30 B channels and 1 D channel in Europe, Asia (except Japan), Australia, and South America. (When PRI includes 30 B channels, channel 0 is used to maintain synchronization and is not counted as either a B or D channel.) The transmission rates for PRI ISDN match the transmission rates for an E1- or T1-carrier line. In North America and Japan, PRI ISDN provides 1.544 Mbps. In other areas, PRI ISDN provides 2.048 Mbps.

In an ISDN connection, the B channels are treated independently. They can be used for simultaneous voice and data; in other words, you can talk on the phone and surf the Web at the same time. For example, if you have an ISDN BRI connection, you can use both channels for data only, or you can use each channel to connect to a different remote office.

The ProCurve Secure Router currently supports ISDN BRI connections. Consequently, this chapter focuses on ISDN BRI.

Elements of an ISDN Connection

All WAN connections, including ISDN lines, consist of three basic elements:

- the physical transmission media, such as the cabling, switches, routers, and other infrastructure required to create and maintain the connection
- electrical signaling specifications for generating, transmitting, and receiving signals through the various transmission media
- Data Link Layer protocols, which provide logical flow control for transmitting data between the two WAN peers (devices at either a connection)

Physical transmission media and electrical specifications are part of the Physical Layer (Layer 1) of the Open Systems Interconnection (OSI) model, and Data Link Layer protocols are part of the Data Link Layer (Layer 2). (See Figure 8-1.)

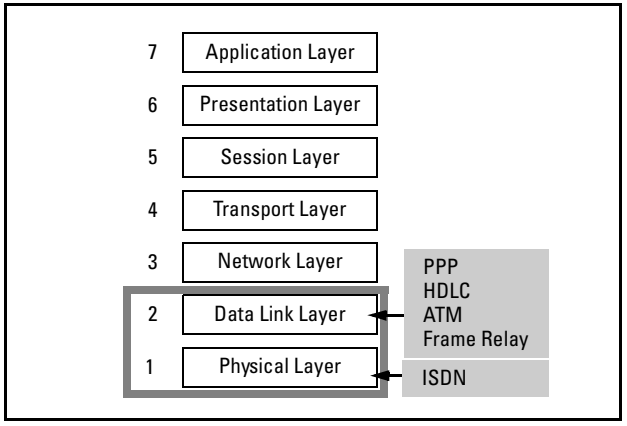

Figure 8-1. Physical and Data Link Layers of the OSI Model

When you configure an ISDN WAN connection, you must configure both the Physical Layer and the Data Link Layer (which is also called the Logical Layer).

The Local Loop

Like other WAN technologies, ISDN connections are provided through public carrier networks. When you lease an ISDN line, your company's equipment must be connected to your public carrier's nearest central office (CO). All of the telecommunications infrastructure—such as repeaters, switches, cable, and connectors—that connects a subscriber's premises to the CO is referred to as the *local loop*.

Because public carrier networks were originally designed to carry analog voice calls, copper wire is the most common physical transmission medium used on the local loop. Copper wire has a limited signal-carrying capacity, making local loops that use copper wire the slowest, least capable component of a WAN connection. ISDN, like DSL, was designed to maximize the limited capability of local loop copper wiring.

ISDN provides integrated voice and data services by means of a fully digital local loop. ISDN is a local-loop-only technology. When ISDN traffic reaches the public carrier's nearest CO, it is converted for transport through the existing public carrier infrastructure.

On the local loop, ISDN requires at least Category 3 (CAT 3) unshielded twisted pair (UTP) cabling. The number of wires required depends on the ISDN service: ISDN BRI requires two wires, or one twisted pair. PRI ISDN requires four wires, or two twisted pairs.

The local loop is divided into two sections by a line of demarcation (demarc), which separates your company's wiring and equipment from the public carrier's wiring and equipment. (See Figure 8-2.) As a general rule, your company owns, operates, and maintains the wiring and equipment on its side of the demarc, and the public carrier owns, operates, and maintains the wiring and equipment on its side of the demarc. For ISDN connections, the position of the demarc varies, depending on which ISDN equipment the public carrier provides.

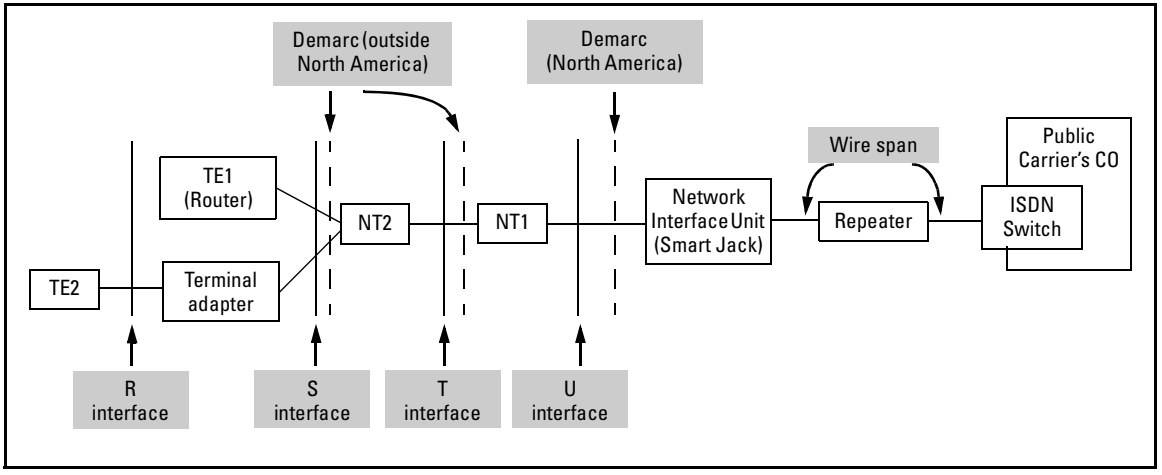

Figure 8-2. ISDN Network

In addition to wire and the demarc, the local loop for an ISDN connection includes:

- ISDN switch—At the public carrier's CO, the ISDN switch multiplexes and de-multiplexes channels on the twisted pair wiring of the local loop. It provides the physical and electrical termination for the ISDN line and then forwards the data onto the public carrier's network.
- Repeater—A repeater receives, amplifies, and retransmits the digital signal so that the signal is always strong enough to be read. Because ISDN lines use 2B1Q coding, which operates at a lower frequency range than T1 or E1 encoding, repeaters are only required every 5.49 km (18,000 feet). In contrast, T1 or E1 encoding requires a repeater approximately every 1.6 km (1 mile or 5,280 feet).
- Network Interface Unit (NIU)—The NIU automatically maintains the WAN connection and enables public carrier employees to perform simple management tasks from a remote location. The NIU is usually located outside the subscriber's premises so that public carrier employees can always access it. (The NIU is commonly referred to as the "smart jack" in North America.)
- Network Termination (NT) 1—The NT1 provides the physical and electrical termination for the ISDN line. It monitors the line, maintains timing, and provides power to the ISDN line. In Europe and Asia, public carriers supply the NT1. In North America, however, the subscriber provides the NT1. In fact, many ISDN vendors are now building the NT1 directly into ISDN equipment such as routers.
- NT2—PRI ISDN also requires an NT2, which provides switching functions and data concentration for managing traffic across multiple B channels. In many regions, the NT1 and NT2 are combined into a single device, which is called an NT12 (NT-one-two) or just NT.
- Terminal equipment (TE) 1—TE1 devices are ISDN-ready devices and can be connected directly to the NT1 or the NT2. TE1 devices include routers, digital phones, and digital fax machines.
- TE2—TE2 devices do not support ISDN and cannot connect directly to an ISDN network. TE2 devices require a terminal adapter (TA) to convert the analog signals produced by the TE2 device into digital signals that can be transmitted over an ISDN connection. TE2 devices include analog telephones and analog fax machines.
- Terminal adapter (TA)—A TA allows you to connect a TE2 device to an ISDN network.

ISDN Interfaces: Connecting Equipment to the ISDN Network

ISDN supports both RJ-11 and RJ-45 connectors. Public carriers typically install an RJ-45 jack to connect the subscriber's premises to the local loop.

You can add equipment at four interface points on the subscriber's side of an ISDN network:

- U interface
- T interface
- S interface
- R interface

These interfaces define the mechanical connectors, the electrical signals, and the protocols used for connections between the ISDN equipment.

U Interface. The U interface provides the connection between the local loop and NT1. For ISDN BRI, the U interface is one twisted pair. For PRI ISDN, the U interface is two twisted pairs.

Because public carriers in Europe and Asia provide the NT1, these regions do not use the U interface. In regions that support the U interface, there can be only one U interface on the ISDN network.

T Interface. The T interface is used to connect the NT1 to the NT2. This interface is a four-wire connection, or two twisted pair. Each pair handles the traffic sent in one direction.

In the United States and Canada, the T interface—along with the NT1 and NT2—is often built into an ISDN device such as a router. In other regions, the T interface is the first interface at the subscriber's premises.

S Interface. The S interface is used to connect the NT2 or the NT1 to the TE1 or TA. This interface is a four-wire connection, or two twisted pair.

On an ISDN BRI connection, all of the TEs or TAs connected to the S interface must take turns transmitting traffic. Because the S interface is a shared medium, the TEs and TAs must be able to detect collisions. PRI ISDN does not support multiple TEs at the S interface.

The S and T interfaces are often combined as the S/T interface.

R Interface. The R interface is used to connect a TE2 device to the TA. Because there are no standards for the R interface, the vendor providing the TA determines how the TA connects to and interacts with the TE2.

Line Coding for ISDN BRI Connections

To provide higher transmission rates on ordinary telephone wire, ISDN BRI uses a compressed encoding scheme called 2B1Q. Essentially, this transmission scheme uses four signal levels, each of which encode one quaternary symbol. A single quaternary symbol, in turn, represents two bits.

The two encoded bits can have up to four different values, each expressed as a different voltage level on the transmission line, as shown in Table 8-1.

Table 8-1. 2B1Q Compressed Line Encoding Scheme

Binary	Quartenary Symbol	Line Voltage
00	-3	-2.5
01	-1	-0.833
10	+3	+2.5
11	+1	+0.833

Note that zero voltage is not a valid signal level.

In addition to compressing data, 2B1Q operates in full duplex mode, allowing data to be transmitted simultaneously in both directions on the local loop.

ISDN Data Link Layer Protocols

As mentioned earlier, the signaling information used to create and maintain ISDN connections is transmitted over the D channel. The ITU Telecommunications Standardization Sector (ITU-T) has defined two protocols for ISDN signaling. These protocols operate at Layer 2 (Data Link Layer) and Layer 3 (Network Layer) of the OSI model:

- Q.921, which is also called Link Access Procedure for D channel (LAPD)
- Q.931

ISDN also supports the following B-channel Data Link Layer protocols:

- Point-to-Point (PPP)
- High-Level Data Link Control (HDLC)
- Frame Relay

LAPD

LAPD establishes the ISDN connection between two endpoints. Exchanged over the D channel, LAPD frames provide the addressing for the dial-up connection, including the service access point identifier (SAPI) and the terminal endpoint identifier (TEI). The SAPI identifies the ISDN service associated with the signaling frame, and the TEI identifies the TE on the subscriber's ISDN line. In addition, LAPD provides error checking and call control.

LAPD frames consist of six main fields. (See Figure 8-3).

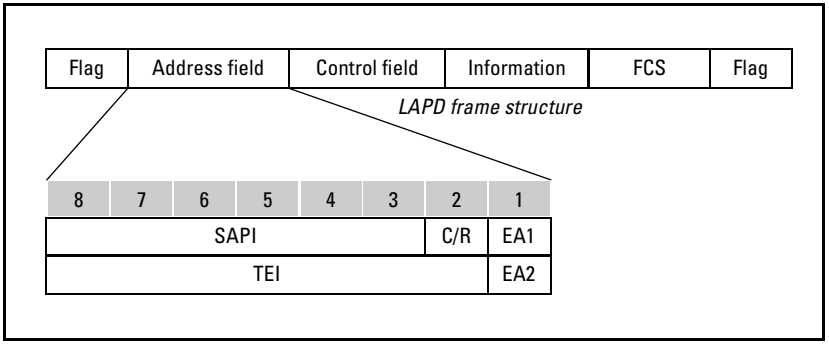

Figure 8-3. LAPD Frame Format

Flag. The flag field is one octet and always has a value of 0x7E.

Address Field. The address field is two octets: In the first octet, the first six bits define the SAPI. The seventh bit is the Command/Response bit (C/R), which designates a command frame or a response frame. The LAPD frame is a command frame:

- when the LAPD frame is from the user and the C/R bit is set to one
- when the frame is from the network and the C/R bit is set to zero,

Other values designate a response frame. The eighth bit is the first address extension bit and is always set to zero.

In the second octet, the first seven bits designate the connection's TEI. TEIs can be assigned statically or dynamically. A statically assigned TEI will have a value between 0 to 63; dynamically assigned TEI range from 64 to 126. A value of 127 designates a broadcast connection meant for all TEs. The eighth bit is the second address extension bit and is always set to one.

Control Field. The third field of an LAPD frame is the control field, which can be either one to two octets. This field identifies the type of frame and contains sequence numbers, control features, and error tracking. The control field identifies the frame as one of the following:

- supervisory frame
- unnumbered frame
- information frame

Information Field. The fourth field of an LAPD frame varies in length and contains the frame's data payload and information. The information field often contains encapsulated Q.931 packets.

FCS Field. The fifth field is the frame check sequence (FCS), which contains a CRC checksum of the address, control, and payload fields.

Flag. The sixth field is a one-octet flag, which signals the end of the frame.

Q.931

The subscriber's ISDN devices and the public carriers devices exchange Q.931 frames to establish, control, and terminate an ISDN call. Q.931 packets are encapsulated in the LAPD frame in the information field.

Call Process

When an ISDN call is placed, the devices go through a procedure to ensure that the connection is made. A basic knowledge of this procedure can help you troubleshoot your ISDN connection. (See Figure 8-4).

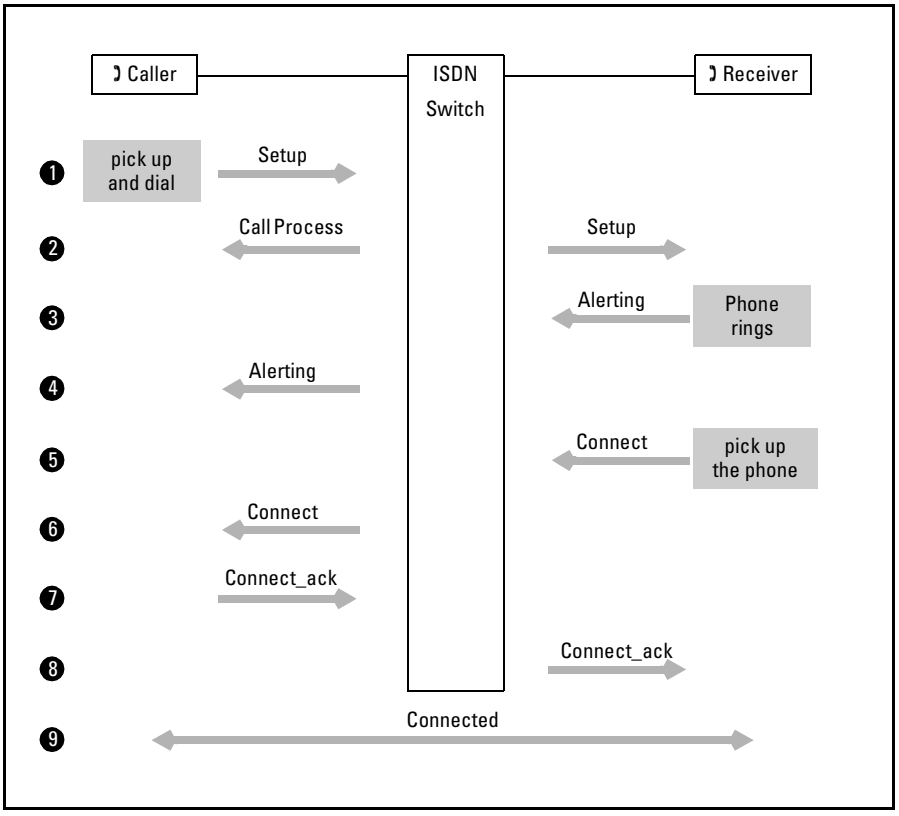

Figure 8-4. ISDN Call Setup Process

Placing a Call. When you use your telephone to place a call, you pick up the phone and get a dialtone, which signals that the phone and voice switch are ready. After you dial a number, your telephone, the public carrier's voice switches, and the receiving phone must exchange frames to establish the connection.

Similarly, when an ISDN modem initiates a connection to another modem, the calling modem, the public carrier's switches, and the receiving modem, must exchange D channel frames. The following is the procedure when placing an ISDN call:

1. The calling modem is activated and sends a SETUP to the switch.
2. If the ISDN switch is available and ready, it sends a CALL PROC to the caller and a SETUP to the receiver.

3. The receiver gets the SETUP. If the receiver is available and ready, it rings the phone and sends an ALERTING message to the switch.
4. The switch forwards the ALERTING to the caller.
5. The receiving ISDN modem sends a CONNECT message to the switch.
6. The switch forwards the CONNECT message to the caller.
7. The caller sends a CONNECT_ACK to the switch.
8. The switch forwards the CONNECT_ACK to the receiver.
9. The call is now connected.

ProCurve Secure Router ISDN Modules

ProCurve Networking offers two types of ISDN modules:

- narrow modules for primary WAN connections
- backup modules for backup WAN connections

Like other narrow modules, the primary ISDN modules fit into the narrow slots on the front of the ProCurve Secure Router. The backup ISDN modules, on the other hand, snap onto the top of narrow modules before those modules are installed into the ProCurve Secure Router. Each narrow module contains a backup port that is enabled for use when a backup module is snapped into place. In fact, the two-port ISDN primary modules contain a backup port, which means you can install a backup module on top of the ISDN primary module.

Both primary and backup ISDN modules provide ISDN BRI connections. However, there are some differences between the modules that may determine which type of modules you purchase for your company's WAN. Some of these differences are listed in Table 8-2.

Table 8-2. Differences Between Primary and Backup ISDN Modules

ISDN Module	Hardware Requirements	Applications	Activation Method	Increasing Bandwidth
primary	uses one narrow slot on the ProCurve Secure Router	primary or backup WAN connection between two offices that exchange data periodically and need a low-cost WAN solution	established only when traffic that you identify as "interesting" needs to be transmitted across the connection	supports Multilink PPP (MLPPP), which can aggregate multiple B channels across different ISDN lines
backup	does not use a narrow slot; installed on top of any narrow module, enabling the use of the backup port on the module	• backup for two locations that must maintain a persistent WAN connection • backup for two locations that require high availability	two activation methods: • persistent backup connection, which is established immediately when the primary connection fails and maintained until the primary connection is re-established • demand routing connection, which is established when two conditions are met: – primary WAN connection fails – traffic you identify as "interesting" needs to be transmitted across the connection	• supports channel bonding with another ProCurve Secure Router when you configure a persistent backup connection • does not support channel bonding with demand routing

Note

Demand routing is supported with the J.04.01 release of the Secure Router operating system (OS).

Both primary and backup ISDN modules use PPP as the Data Link Layer protocol for the WAN connection and support PPP authentication. This chapter describes how to configure and manage ISDN connections established through the primary ISDN modules. For more information about backup modules, see the *Advanced Management and Configuration Guide*, *Chapter 3: Configuring Backup WAN Connections*.

Primary ISDN Modules

For primary WAN connections, ProCurve Networking currently offers two types of modules:

- ISDN BRI U module—used in the United States and Canada
- ISDN BRI S/T module—used in all other countries

Both of these ISDN modules support the following standards:

- National ISDN-1—Defined in the mid 1990s by the National Institute of Standards and Technology (NIS) and Bellcore (now called Telcordia), National ISDN-1 outlines a common set of options that ISDN manufacturers and public carriers must provide.
- Northern Telecom Digital Multiplex System (DMS)-100—DMS-100 is another standard for transmitting voice and data over an ISDN line.
- AT&T 5ESS—AT&T switches use Lucent signaling.

In addition, the ISDN BRI S/T module supports:

- Euro-ISDN—Also called Normes Européennes de Télécommunication 3 (NET3), Euro-ISDN was defined in the late 1980s by the European Commission so that equipment manufactured in one country could be used throughout Europe.

Note

Because the two-port ISDN modules have a single TDM clock, you cannot use one module to connect to two separate service providers. If you lease ISDN lines from two different service providers, you will need to use two separate ISDN modules—either 2 two-port ISDN modules or 1 two-port ISDN module and one ISDN backup module.

Table 8-3 lists the supported ISDN switches, the classifications, and electrical standards for each ISDN module.

Table 8-3. Supported ISDN Standards

Type	Switch Types	Classifications	Electrical
ISDN BRI S/T module	• National ISDN-1 • Northern Telecom DMS-100 • AT&T 5ESS • DSS1 ETSI Euro-ISDN	• ACIF S031 • ETSI TBR 3 • EN 60950 • IEC 60950 • AS/NZS 60950 • V.54 loopback support	• FCC Part 15 Class A • EN 55022 Class A • EN 55024 • EN 61000-3-2 • EN 61000-3-3
ISDN BRI U module	• National ISDN-1 • Northern Telecom DMS-100 • AT&T 5ESS	• ACTA/FCC Part 68 • IC CS-03 • UL/CUL 60950 • V.54 loopback support	• FCC Part 15 Class A • EN 55022 Class A • EN 55024 • EN 61000-3-2 • EN 61000-3-3

Using Demand Routing for ISDN Connections

When you lease an ISDN line, you pay only for the time when the connection is established. If no one is sending traffic that must be transmitted over the dial-up WAN connection, you do not want the connection to be up. However, as soon as a user sends data that must be transmitted over the dial-up WAN connection, you want that connection to be established immediately.

When you purchase primary ISDN modules for the ProCurve Secure Router, you configure demand routing to manage the ISDN connection so that when traffic is sent from one site to another the dial-up connection is established. For example, you might lease an ISDN line to connect a branch office to the main office. When a workstation at the branch office sends a packet that must be forwarded to the main office, demand routing triggers the ISDN connection and ensures that the traffic is forwarded across the established link. If no more traffic is transmitted from the branch office to the main office, demand routing ensures that the ISDN connection is terminated until it is required again. (See Figure 8-5.) If you configure demand routing correctly, you can minimize the amount your company pays for its ISDN connection.

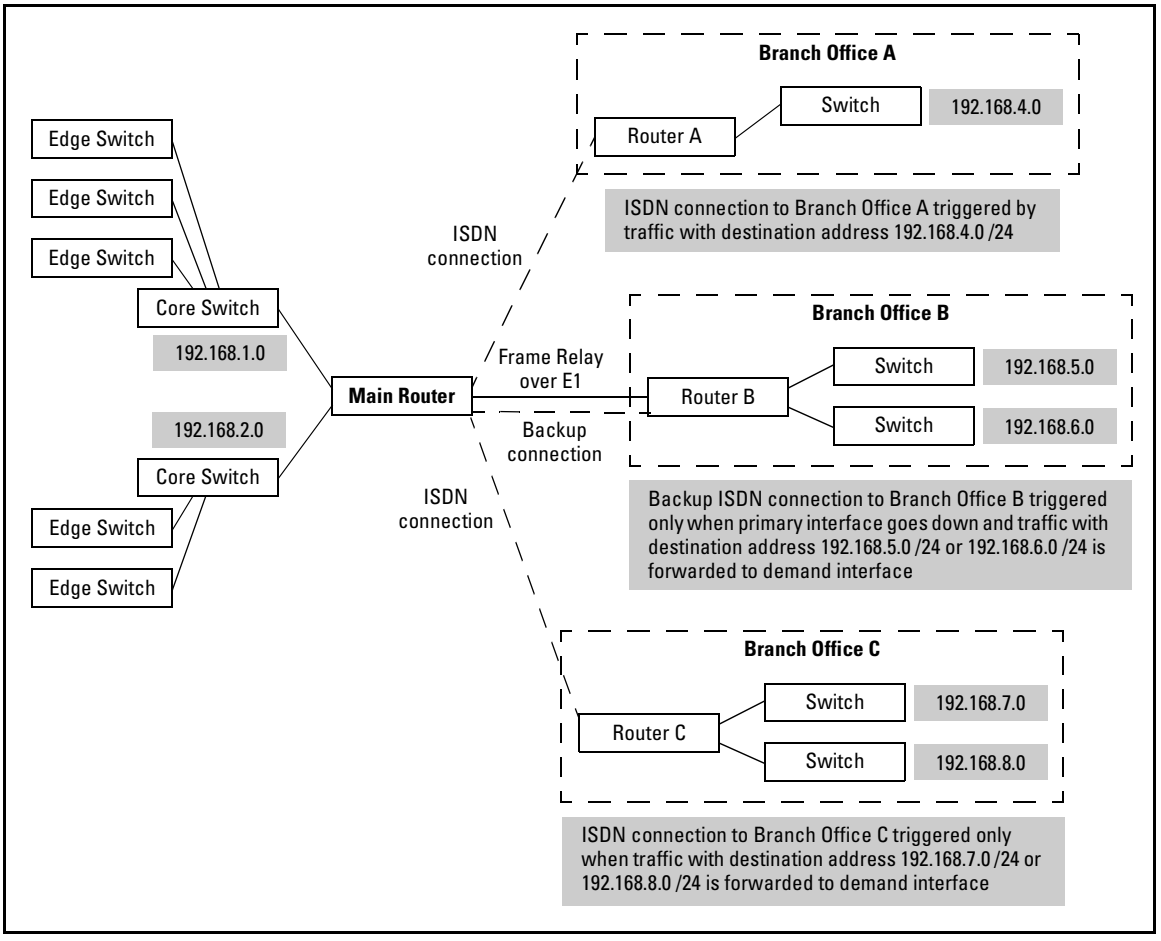

Figure 8-5. Using Demand Routing to Establish Dial-Up Connections for Primary and Backup Interfaces

Demand routing can also be used for backup dial-up connections, ensuring that they are established only when the primary interface is down and traffic must be transmitted to another site. (For more information about using demand routing for backup dial-up connections, see the *Advanced Management and Configuration Guide*, *Chapter 3: Configuring Backup WAN Connections*.)

To configure demand routing for a primary ISDN module, you must complete the following steps:

1. Create an extended access control list (ACL) to define the traffic that will trigger the dial-up connection.
2. Configure a demand interface.
3. Configure the BRI interface.
4. Configure an ISDN group.
5. Create a static route to the far-end network.

Define the Traffic That Triggers the Connection

When configuring demand routing, you must define the interesting traffic—the traffic that triggers, or activates, the WAN connection. For example, if you are configuring demand routing for an ISDN connection between the main office and a branch office, the interesting traffic would be the packets destined for the branch office. (See Figure 8-6.)

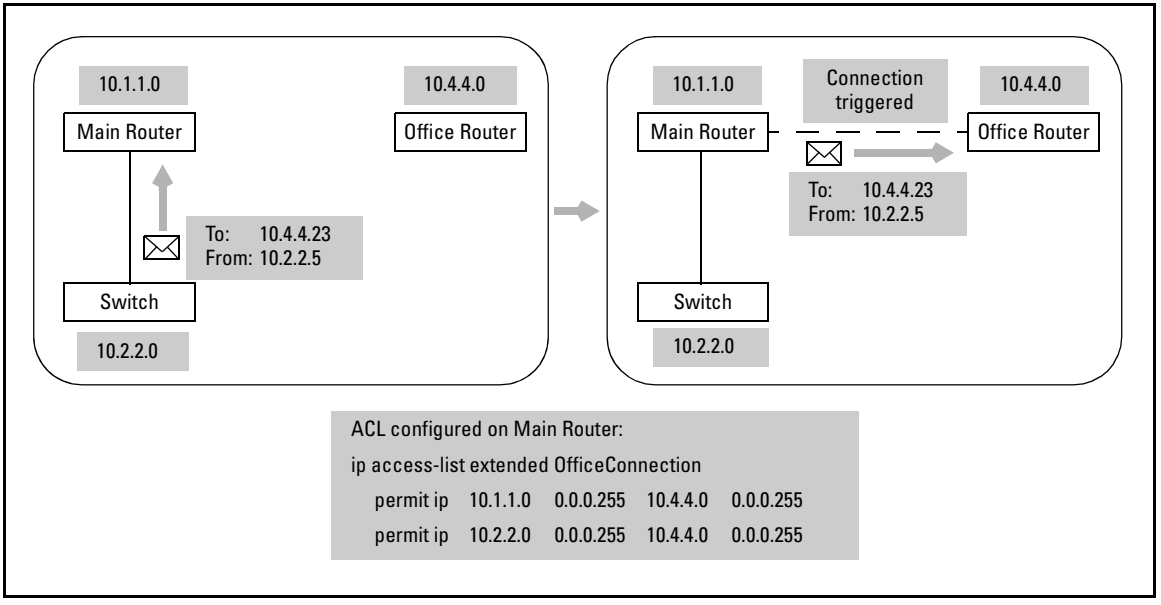

Figure 8-6. Connection Triggered When Interesting Traffic Is Received on a Router Interface

To define the interesting traffic, you create an extended ACL. The ProCurve Secure Router will use this ACL to identify and select traffic that triggers a dial-up connection.

From the global configuration mode context, enter:

Syntax: ip access-list extended <*listname*>

Replace ***<listname>*** with an alphanumeric descriptor that is meaningful to you. The listname is case sensitive.

After you enter this command, you are moved to the extended ACL configuration mode context, as shown below:

```
ProCurve(config-ext-nacl)#
```

You can now enter permit statements to define the traffic that will trigger the dial-up connection. Use the following command syntax:

Syntax: [permit | deny] <*protocol*> <*source address*> <*source port*> <*destination address*> <*destination port*> [log | log-input]

You must specify a ***<protocol>***, ***<source address>***, and ***<destination address>***. However, the following are optional:

- ***<source port>*** for TCP or UDP traffic
- ***<destination port>*** for TCP or UDP traffic
- **[log | log-input]**

Specifying a Protocol

When you create a permit or deny statement for an extended ACL, you must always specify a protocol. Valid protocols include:

- AHP
- ESP
- GRE
- ICMP
- IP
- TCP
- UDP

You can also specify the number of the protocol. Valid numbers include any number between 0 and 255.

For demand routing, you might want to create an ACL that selects all of the traffic to a particular subnet. In this case, you should specify **ip** as the protocol.

Defining the Source and Destination Addresses

When you create an extended ACL, you must configure both a source and a destination address for each entry. You specify the source address first and then you specify the destination address.

To specify the source address and the destination address, use the following syntax:

[any | host {<*A.B.C.D*> | <*hostname*>} | <*A.B.C.D*> <*wildcard bits*>]

Table 8-4 lists the options you have for specifying both the source address and the destination address.

Table 8-4. Options for Specifying Source and Destination Addresses in an ACL

Option	Meaning
any	match all hosts
host [<A.B.C.D> | <hostname>]	specify a single IP address or a single host
<A.B.C.D> <wildcard bits>	specify a range of IP addresses

For example, you may want any traffic to the far-end network to trigger the dial-up connection. If the far-end network has a network address of 192.168.115.0 /24, enter:

```
ProCurve(config-ext-nacl)# permit ip any 192.168.115.0 0.0.0.255
```

If you want any outbound traffic from a particular network segment to trigger a dial-up connection, enter:

```
ProCurve(config-ext-nacl)#  permit ip 192.168.1.0 0.0.0.255 any
```

You might want the IP traffic from a specific host to a specific destination to trigger an ISDN connection. In this case, enter:

```
ProCurve(config-ext-nacl)# permit ip host 192.168.1.1 host 192.168.115.100
```

Using Wildcard Bits. You use wildcard bits to permit or deny a range of IP addresses. Wildcard bits determine which bits in the specified address the Secure Router OS should match to a packet and which address bits it should ignore. When you enter wildcard bits, you use a 0 to indicate that the Secure

Router OS should match the corresponding bit in the IP address. You use a 1 to indicate that the Secure Router OS should ignore the corresponding bit in the IP address. In other words, the Secure Router OS does not have to match that bit.

For example, you might enter:

```
ProCurve(config-ext-nacl)# deny ip any 192.115.1.0 0.0.0.255
```

Essentially, you use the wildcard bits to specify the subnet that you want the Secure Router OS to match for a particular packet field (such as the source address). For example, if you enter 192.115.1.90 with the wildcard bits 0.0.0.255, the Secure Router OS will not match any address bits in the fourth octet of the IP address. The Secure Router OS will match incoming packets to the IP subnet address 192.115.1.0 /24 (because it will not match the bits in the fourth octet). (See Figure 8-7.)

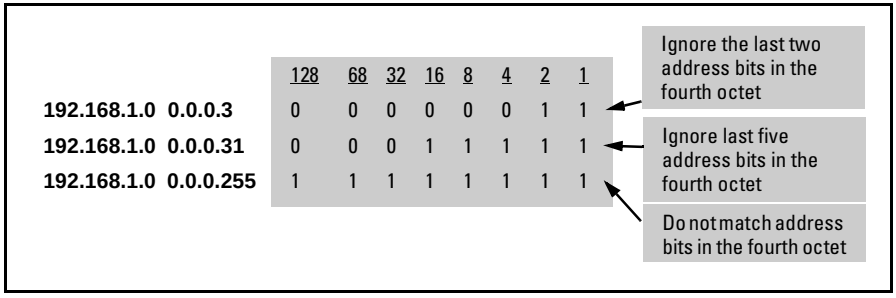

Figure 8-7. Understanding Wildcard Bits

Implicit "Deny Any" Entry. Each ACL includes an implicit "deny any" entry at the end of the list. If a packet does not match any entry in the ACL you create, it matches the implicit "deny any" entry.

When you configure an ACL to select interesting traffic, you should permit at least one host. Otherwise, you will, in effect, prevent the dial-up connection from becoming active.

Log. Include the **log** option if you want the Secure Router OS to log a message:

- when **debug access-list** is enabled for this ACL
- when a packet matches this ACL

For example, a log will be generated when a packet triggers the dial-up connection.

Exit the ACL. After you have finished creating the ACL, enter **exit** to return to the global configuration mode context, as shown below:

```
ProCurve(config-ext-nacl)# exit
ProCurve(config)#
```

After you create the ACL, you must apply it to the demand interface. In fact, the ACL will have no effect until you apply it to the demand interface. (For more information about configuring ACLs, see the *Advanced Management and Configuration Guide*, *Chapter 5: Applying Access Control to Router Interfaces*.)

Configuring the Demand Interface

You must create a demand interface for each router to which the ProCurve Secure Router will connect through a dial-up connection. The demand interface provides the Data Link Layer for the physical dial-up interface.

Like other logical interfaces such as Frame Relay or PPP, the demand interface controls the logical functions for the WAN connection. In many ways, you configure the demand interface as you do any other logical interface. For example, you assign the demand interface an IP address. From this interface, you apply the ACL that defines the interesting traffic that triggers the dial-up WAN connection. You can also apply other ACLs or an access control policy (ACP) to this interface if you want to block certain traffic from being transmitted over the connection.

The demand interface is different from other logical interfaces, however. For one thing, the demand interface is not bound to a specific physical interface or interfaces. Instead, the demand interface is associated with a pool of physical interfaces.

The demand interface must also handle its status differently: it must always be up, whether or not the physical dial-up interface associated with the demand interface is up. Because the demand interface cannot actually be up if the Physical Layer is down, it “spoofs” an up state. As a result, the demand interface can be listed as a directly connected interface in the router’s routing table, even when the dial-up interface is not in use.

Because the demand interface spoofs an up state, you can add routes to networks reached through the dial-up connection managed by the demand interface. The demand interface is the forwarding interface for these routes.

When the ProCurve Secure Router detects traffic that must be routed through a demand interface, it processes the extended ACL applied to the demand interface to define the interesting traffic. If the traffic matches that ACL, the router attempts to establish the ISDN connection.

After the physical ISDN connection is established, the ProCurve Secure Router uses PPP to set up the Data Link Layer. To ensure that only authorized routers establish ISDN connections to your router, you should configure PPP authentication for the dial-up connection.

To configure the demand interface, complete the following steps:

1. Create a demand interface.
2. Configure an IP address for the demand interface.
3. Apply the ACL that defines interesting traffic to the demand interface.
4. Specify whether the demand interface can originate a call, answer a call, or both.
5. Create a resource pool.
6. Configure instructions for placing a call by entering **connect-sequence** commands.
7. Configure timers, caller, and hold queue settings (optional).
8. Configure caller settings (optional).
9. Configure PPP authentication (optional but recommended).

You must complete steps 1-6. Steps 7-9 are optional.

Creating the Demand Interface

To create a demand interface and access the demand interface configuration mode context, enter the following command from the global configuration mode context:

Syntax: interface demand <*number*>

Replace ***<number>*** with a number between 1 and 1024 for this demand interface. You should configure a different demand interface for each connection to a remote site or device, and each demand interface must have a unique number.

Like loopback interfaces, demand interfaces do not have to be activated. That is, you do not have to enter **no shutdown**. After you create the demand interface, its status automatically changes to administratively up. The demand interface will begin spoofing an up status after you configure an IP address for it.

Shut Down the Demand Interface. You may need to shut down the demand interface. For example, you may need to shut down the interface to correct a configuration setting or to troubleshoot a problem with the ISDN line. Enter:

```
ProCurve(config-demand 1)# shutdown
```

To activate the interface again, enter:

```
ProCurve(config-demand 1)# no shutdown
```

Configuring an IP Address

Because the demand interface uses PPP as the Date Link Layer protocol, you have several options for setting up an IP address: you can assign the demand interface a static IP address, you can configure it to negotiate the IP address from its PPP peer, or you can configure it as an unnumbered interface.

Configure a Static IP Address. To assign the demand interface a static IP address, enter:

Syntax: ip address <*A.B.C.D*> <*subnet mask* | /*prefix length*>

For example, you might enter:

```
ProCurve(config-demand 1)# ip address 10.10.10.1 255.255.255.252
```

or

```
ProCurve(config-demand 1)# ip address 10.1.1.1 /30
```

Configure a Negotiated IP Address. If you want the demand interface to negotiate an IP address with its PPP peer, enter the following command from the demand interface configuration mode context:

Syntax: ip address negotiated

Configure the Demand Interface as an Unnumbered Interface. To conserve IP addresses on your network, you may want to create the demand interface as an unnumbered interface. When you assign a logical interface on the router an IP address, that IP address cannot overlap with the IP addresses assigned to other logical interfaces. As a result, each interface that has an IP address represents an entire subnet. Depending on the subnetting scheme you use, you may not have enough IP addresses to assign to each active interface on your router.

To conserve IP addresses, you may want the demand interface to use the IP address of another interface. However, if the interface to which the IP address is actually assigned goes down, the demand interface will be unavailable as well. Because there is little chance that a loopback interface will go down, you may want to assign the IP address to a loopback interface.

To configure the demand interface as an unnumbered interface, enter the following command from the demand interface configuration mode context:

Syntax: ip unnumbered <*interface ID*>

Valid interfaces from which the demand interface can takes its address include:

- Ethernet interfaces and subinterfaces
- Frame Relay subinterfaces
- PPP interfaces
- loopback interfaces
- Asynchronous Transfer Mode (ATM) subinterfaces

For example, you would enter the following commands to configure a loopback interface and then configure the demand 1 interface to use the IP address assigned to that loopback interface:

```
ProCurve(config)# interface loopback 1
ProCurve(config-loop 1)# ip address 192.168.115.1 /24
ProCurve(config-loop 1)# interface demand 1
ProCurve(config-demand 1)# ip unnumbered loopback 1
```

Spoofing. After you configure an IP address for the demand interface, its status should change to “up (spoofing),” and it should be listed as a directly connected interface in the routing table. To check the status of the demand interface, use the **do** command to enter a **show** command from the demand interface configuration mode context:

```
ProCurve(config-demand 1)# do show interface demand 1
```

To view the routing table, enter:

ProCurve(config-demand 1)# do show ip route

Figure 8-8 shows a routing table that includes demand interface 1, a directly connected interface.

```
C    10.2.2.0/30 is directly connected, ppp 1
C    10.3.3.0/30 is directly connected, demand 1
C    192.168.20.0/24 is directly connected, eth 0/1
```

Figure 8-8. Routing Table That Includes a Demand Interface

Matching the Interesting Traffic

To finish defining the interesting traffic that will trigger a dial-up connection, you must associate the ACL you created with the demand interface. From the demand interface configuration mode context, enter:

Syntax: match-interesting [list | reverse list] <*listname* > [in | out]

Include the **list** option if you want the ProCurve Secure Router to use standard matching logic for the ACL. That is, the router will try to match the packet's source address to the source address that is defined in the extended ACL. Likewise, the router will try to match the packet's destination address with the destination address that is defined in the extended ACL.

Include the **reverse list** option if you want the ProCurve Secure Router to use reverse matching logic when processing the ACL. The ProCurve Secure Router will use the ACL to match traffic that is transmitted in the opposite direction, eliminating the need to create another ACL for the traffic inbound on the WAN connection. The router will try to match the packet's source address with the destination address that is defined in the ACL. The router will then try to match the packet's destination address with the source address that is defined in the ACL.

Replace ***<listname>*** with the ACL that you created to define the interesting traffic. You can specify only extended ACLs.

Including **in** or **out** is optional. By default, the ProCurve Secure Router uses the ACL you specify to check both incoming and outgoing traffic. If you do not specify a direction, outbound traffic is matched to the specified ACL, and inbound traffic is matched to the reverse of the ACL.

If you include the **in** option when you enter the **match-interesting** command, the ProCurve Secure Router will check only the traffic received on the demand interface. If you include the **out** option, the router will check only the traffic transmitted from the interface.

For example, suppose that you configured the Branch ACL to select traffic from the local network destined to a branch office network. If you want both traffic outbound to the branch office and inbound from the branch office to trigger the dial-up connection, apply the Branch ACL to demand 1 interface:

```
ProCurve(config-demand 1)# match-interesting list Branch
```

When you view the demand interface in the running-config, you will see two commands, even though you entered only one. (See Figure 8-9.)

```
interface demand 1
   match-interesting list Branch out
   match-interesting reverse list Branch in
```

Figure 8-9. The match-interesting Command as Displayed in the Running-Config

Entering the following two commands would accomplish the same thing:

```
ProCurve(config-demand 1)# match-interesting list Branch out
ProCurve(config-demand 1)# match-interesting reverse list Branch in
```

Note

After you configure demand routing, you should monitor usage of the dial-up connection to determine if you have correctly configured the ACL to select interesting traffic. To avoid any problems when the bill for the dial-up connection arrives, ensure that the connection is being triggered only when you want it to be. To minimize costs, you may need to change the ACL by further limiting the traffic that triggers the connection.

Applying an ACP or Another ACL to the Demand Interface. In addition to using an ACL to determine which traffic triggers a dial-up connection, you can use ACLs to control incoming traffic and outgoing traffic on that connection. You have two options for controlling traffic:

- You can apply ACLs directly to the demand interface. If you choose this option, you can apply one ACL directly to the interface to control incoming traffic, and you can apply another ACL directly to the interface to control outgoing traffic. (For best practices, you typically apply an extended ACL closest to the source of incoming traffic so that you do not waste the router's processing time on traffic that will ultimately be discarded.)

- You can apply an access control policy (ACP) to the demand interface. ACPs control incoming traffic and can contain multiple ACLs.

You use the **ip access-group command** to apply ACLs directly to the demand interface, or you use the **access-policy** command to apply an ACP to the demand interface. (For more information about using ACLs separately or in combination with ACPs, see *Chapter 5: Applying Access Control to Router Interfaces*.) The ProCurve Secure Router will match traffic to the ACLs or the ACP to control access to an already-active backup connection. However, the connection will only be *triggered* by traffic that matches the ACL that you specify in the **match-interesting list** command.

Because you can configure one ACL to trigger the dial-up connection and another ACL to control access to the dial-up connection, you can allow certain types of traffic to use a connection only when it is already established. For example, if you apply an ACL for outbound traffic to the demand interface, the router will match traffic destined out the demand interface against this list first. If the router determines that a packet is allowed, it will then check the ACL specified with the **match-interesting list** command to determine if the packet should trigger the backup connection. If the packet is not defined as interesting traffic, the ProCurve Secure Router will not attempt to establish the connection. However, if the connection is already established, the router will transmit packets that are permitted by the ACL, but not selected as interesting traffic, over the ISDN link. These packets will *not* reset the idle timer for the demand interface. (The idle timer determines how long the dial-up connection will remain connected in the absence of interesting traffic. When the router receives interesting traffic, it resets the idle timer. For more information about timers, see “Configuring the idle-timeout Option” on page 8-37 and “Configuring the fast-idle Option” on page 8-38.)

For example, suppose two nodes at a remote site need to communicate with a server at a local site. One node is specified in the ACL that triggers the connection, but the other node is not. The first node’s communication will keep the link active until it has completed its transfer of data and the idle timer has expired. If the idle timer expires when the second node is communicating with the server, the connection will be terminated because the second node’s traffic does not match the ACL specified in the **match-interesting list** command.

In addition to applying an ACL to control outbound traffic, you can apply an ACL for inbound traffic or an ACP to the demand interface. In this case, the ACL or the ACP will filter inbound traffic to your network over the backup connection. If the router determines that a packet is allowed, it will forward

the packet. However, the router will reset the dial-up connection's idle timer only if the packet also matches the ACL specified with the **match-interesting reverse list** command.

Specifying the connect-mode Option

You can control whether the demand interface can be used to originate a call, answer a call, or both. From the demand interface configuration mode context, enter:

Syntax: connect-mode [originate | answer | either]

Table 8-5 shows each option and when you would use it. The default setting is **either**.

Table 8-5. Options for the connect-mode Command

Option	Explanation
originate	The demand interface can make calls but cannot answer them.
answer	The demand interface can answer calls but cannot make them.
either	The demand interface can make calls and answer them.

No matter what you configure as interesting traffic, the **connect-mode** command controls whether or not the demand interface can originate or answer a call. When the demand interface receives outbound interesting traffic, it will originate a connection only if the connect mode you configured for the demand interface allows it to originate a call.

If a demand interface receives outbound interesting traffic and a dial-up connection is already established on this interface, the ProCurve Secure Router resets the idle timer on the connected link. (The idle timer determines how long the ISDN connection can remain up if no traffic is transmitted over it.) The router also resets the idle timer when it receives inbound interesting traffic through the demand interface.

If you want the demand interface to originate a call when it receives interesting traffic, you must set the **connect-mode** to **originate** or **either**. You could also configure the demand interface so that an ACL selects outbound traffic (**match-interesting list <*listname*>**) but the **connect-mode** command is set to **answer**. In this mode, the outbound traffic will not trigger a connection, but it will keep the connection up after the demand interface answers a call.

Note

Currently, it is not possible to have outbound traffic that will originate a call but not keep the link up. Because the **match-interesting** command controls both the traffic that triggers a connection and the traffic that resets the idle timer, any outbound interesting traffic that initiates a connection also keep the link up.

To return the connect-mode to its default setting of **either**, enter:

```
ProCurve(config-demand 1)# no connect-mode
```

Associating a Resource Pool with the Demand Interface

Rather than using a **bind** command to create a persistent, one-to-one connection between the demand interface and a physical interface, you use the **resource pool** command to link the demand interface to one or multiple ISDN BRI interfaces. The **resource pool** command creates a resource pool and associates it with a particular demand interface. Each demand interface can be associated with only one resource pool.

To create a resource pool and associate it with the demand interface, enter:

```
ProCurve(config-demand 1)# resource pool <poolname>
```

Replace ***<poolname>*** with the name of the resource pool that contains the physical interfaces that this demand interface will use to originate or answer connections.

This resource pool is empty until you assign members to it. For primary ISDN connections, you will assign an ISDN group to the resource pool. You must be at the configuration mode context for the ISDN group. (For more information, see “Configuring the ISDN Group” on page 8-44.)

Defining the Connect Sequence

You must configure a connect sequence to specify:

- the telephone number that the demand interface dials to connect to the other site
- the type of dial-up connection to establish

When the ProCurve Secure Router detects interesting traffic and no connections are currently established to carry this traffic, it uses a connect sequence to try to establish a connection. This process is called an *activation attempt*.

You can configure more than one connect sequence for a demand interface. For example, you may want to configure more than one connect sequence if the main office has more than on ISDN line. Then, if one ISDN line is in use, the ProCurve Secure Router can dial another line to establish a connection. You may also want to configure more than one connect sequence to connect to a different router at the main office. Then if one router at the main office is down, the router at a branch office can still connect to the main office.

To configure a connect sequence, enter the following command from the demand interface configuration mode context:

Syntax: connect-sequence <s*equence-number*> dial-string <*string*> [<*resource-type*>] [busyout-threshold <*value*>]

Replace ***<sequence-number>*** with a number between 1 and 65535 to identify this set of connection instructions.

Replace ***<string>*** with the telephone number that the demand interface should dial to make the connection.

Replace ***<resource-type>*** with one of the options listed in Table 8-6. The option you enter will limit this connection to a particular type of dial-up connection.

Table 8-6. Defining a Resource Type for a Connect Sequence

Option	Description
isdn-64k	Any dial resource can be used, but if ISDN is used, the call must be placed using a 64-Kbps channel.
isdn-56k	Any dial resource can be used, but if ISDN is used, the call must be placed using a 56-Kbps channel.
forced-analog	Only analog resources can be used. (This option is used when you configure demand routing with a backup analog line.)
forced-isdn-64k	Only ISDN resources can be used, and the call must be placed using a 64-Kbps channel.
forced-isdn-56k	Only ISDN resources can be used, and the call must be placed using a 56-Kbps channel.

Because you are setting up a connect sequence for an ISDN connection, you should enter the **forced-isdn-64k** or **forced-isdn-56k** options, depending on the speed of the B channel. Your service provider should tell you which option to use.

Specifying the **busyout-threshold <*value*>** is optional. Include a value to specify the maximum number of times the ProCurve Secure Router will try this connect sequence in a single call attempt. If you specify 0, the ProCurve Secure Router will make an unlimited number of attempts. If you specify any other number, the ProCurve Secure Router will skip this connect sequence after it reaches the maximum number. (Depending on your configuration, the ProCurve Secure Router may cycle through the list of connect sequences more than once in its attempt to establish a connection. For more information, see "Configure the Number of Connect Sequence Attempts" on page 8-33.)

There is no default connect sequence. If you do not enter at least one **connect-sequence** command, the demand interface will not be able to originate a dial-up connection.

Deleting a Connect Sequence. To delete a connect sequence entry, enter the following command from the demand interface configuration mode context:

Syntax: no connect-sequence <*sequence-number*>

Specify the Order in Which Connect Sequences Are Used

If you enter more than one **connect-sequence** command, you can configure the order in which each connect sequence is used. From the demand interface configuration mode context, enter:

Syntax: connect-order [sequential | last-successful | round-robin]

Table 8-7 lists each option with a brief description.

Table 8-7. Options for Processing the Connect Sequences

Option	Description
sequential	Process each connect sequence in numerical order, starting with the lowest number and ending with the highest number.
last-successful	Process the last-successful connect sequence first. If that connect sequence is not successful, process those remaining in numerical order, starting with the lowest number and ending with the highest number.
round-robin	First, process the connect sequence that follows the last-successful connect sequence. If that connect sequence fails, process the next highest sequence. (If no connection has been made, process the first connect sequence.)

The default setting is **sequential**.

Returning to the Default Connect Sequence Processing Order. To return the **connect-order** command to its default setting of **sequential**, enter:

```
ProCurve(config-demand 1)# no connect-order
```

Configure the Number of Connect Sequence Attempts

You can limit the number of times that the ProCurve Secure Router processes the connect sequences configured for a demand interface if it is unable to establish a connection. The router will process the connect sequences in the order you specify (with the **connect-order** command). If the router processes all of the connect sequences and is unable to establish a connection, the router has made one connect sequence attempt. (Note that in one attempt, the router can retry a particular connect sequence as many times as specified for that connect sequence's **busyout-threshold** setting.) The router then repeats the process until it reaches the number that you have specified in the **connect-sequence attempts** command.

From the demand interface configuration mode context, enter:

Syntax: connect-sequence attempts <*value*>

Replace ***<value>*** with the number of times the ProCurve Secure Router will cycle through the connect sequences specified for a demand interface. You can specify a number between 0 and 65535. The default setting is 1. Specifying 0 places no limit on the number of attempts.

Configure Settings for the Recovery State

When the ProCurve Secure Router tries to establish a connection, one of the following conditions will result:

A BRI Interface Is Available, and the Call Is Connected. If the ProCurve Secure Router successfully establishes a physical connection (Layer 1), it will begin to negotiate a PPP session with the far-end router.

No BRI Interfaces Are Available. If no BRI interface in the associated resource pool is available for use, the ProCurve Secure Router places all interfaces in the resource pool in fast-idle mode, which decreases the amount of time an interface can remain idle before the router disconnects the ISDN connection. The router then monitors the BRI interfaces until one becomes

available. If a BRI interface becomes available, the ProCurve Secure Router uses that interface to dial a connect-sequence. At the same time, the router cancels the fast-idle mode for the resource pool. (For more information about fast-idle mode, see "Configuring the fast-idle Option" on page 8-38.)

A BRI Interface Is Available, But the Call Fails. If a BRI interface is available and the ProCurve Secure Router attempts to establish a connection, the call may fail for a number of reasons: a busy signal, no answer, connection timeout, and so on. When a connection attempt fails, the router increments the failure count for that connect sequence and then tries to use the next connect sequence to establish a dial-up connection. The **busyout-threshold** option determines the number of times the ProCurve Secure Router processes a particular connect sequence during each connect sequence attempt.

For example, if connect sequence 10 has a busyout-threshold of 3 and connect sequence 11 has a busyout-threshold of 2, the router will process connect sequence 10 three times and connect sequence 11 twice (alternating between the two sequences). If, at the end of the five total attempts, the router cannot establish a connection, it has made one connect sequence attempt.

If the router reaches the maximum number of connect sequence attempts, the ProCurve Secure Router will, by default, change the status of the demand interface to "DOWN (recovery active)." The router will remove the IP address from the demand interface and any associated routes from the routing table. No interesting traffic will be forwarded to the demand interface. If you have configured an alternate route for traffic, the ProCurve Secure Router will activate and use that route.

While the demand interface is in this recovery active state, the ProCurve Secure Router will periodically process the connect sequences and try to establish a dial-up connection. If the router can successfully establish a connection, it will change the status of the demand interface to up, reinstate the routes through the interface, and begin forwarding interesting traffic to the demand interface.

However, if the ProCurve Secure Router cannot establish a connection, it will, by default, continue to try the connect sequences every 120 seconds. You can change the default settings for the recovery mode: you can configure how often the ProCurve Secure Router attempts to establish a connection and the number of attempts it makes in the recovery mode. From the demand interface configuration mode context, enter:

Syntax: connect-sequence interface-recovery retry-interval <*seconds*> max-retries <*number*>

Replace <***seconds***> with the number of seconds you want the demand interface to wait between connect sequence attempts. You can specify a number between 1 and 65535. The default setting is 120 seconds.

Replace ***<number>*** with a number between 0 and 65535. If you specify 0, the ProCurve Secure Router will continue to try to establish a connection until it is successful or you clear the interface. The number you specify overrides the **connect-sequence attempts** setting while the demand interface is in recovery mode. The default setting is 0, or unlimited. That is, the demand interface remains in recovery mode until it successfully establishes a call or until you shutdown the interface.

To disable the recovery mode, enter the following command from the demand interface configuration mode context:

```
ProCurve(config-demand 1)# no connect-sequence interface-recovery
```

Understanding How the connect-sequence Commands Work

Before you configure all the settings for connect sequences, you should understand how these settings interrelate. For example, consider the configuration shown in Figure 8-10:

```
interface demand 1
  connect-order sequential
  connect-sequence attempts 3
  connect-sequence 10 dial-string 5551212 forced-isdn-64k busyout-threshold 3
  connect-sequence 20 dial-string 5552222 forced-isdn-64k busyout-threshold 1
  connect-sequence interface-recovery retry-interval 60 max-retries 5
  resource pool Pool
```

Figure 8-10. Connection Instructions for a Demand Interface

The resource pool for this demand interface contains two BRI interfaces. If interesting traffic is forwarded to this demand interface, the ProCurve Secure Router will first process connect sequence 10 (because the **connect-order** is **sequential**). If the BRI interface is available, the ProCurve Secure Router will try to call 5551212. (See Figure 8-11.)

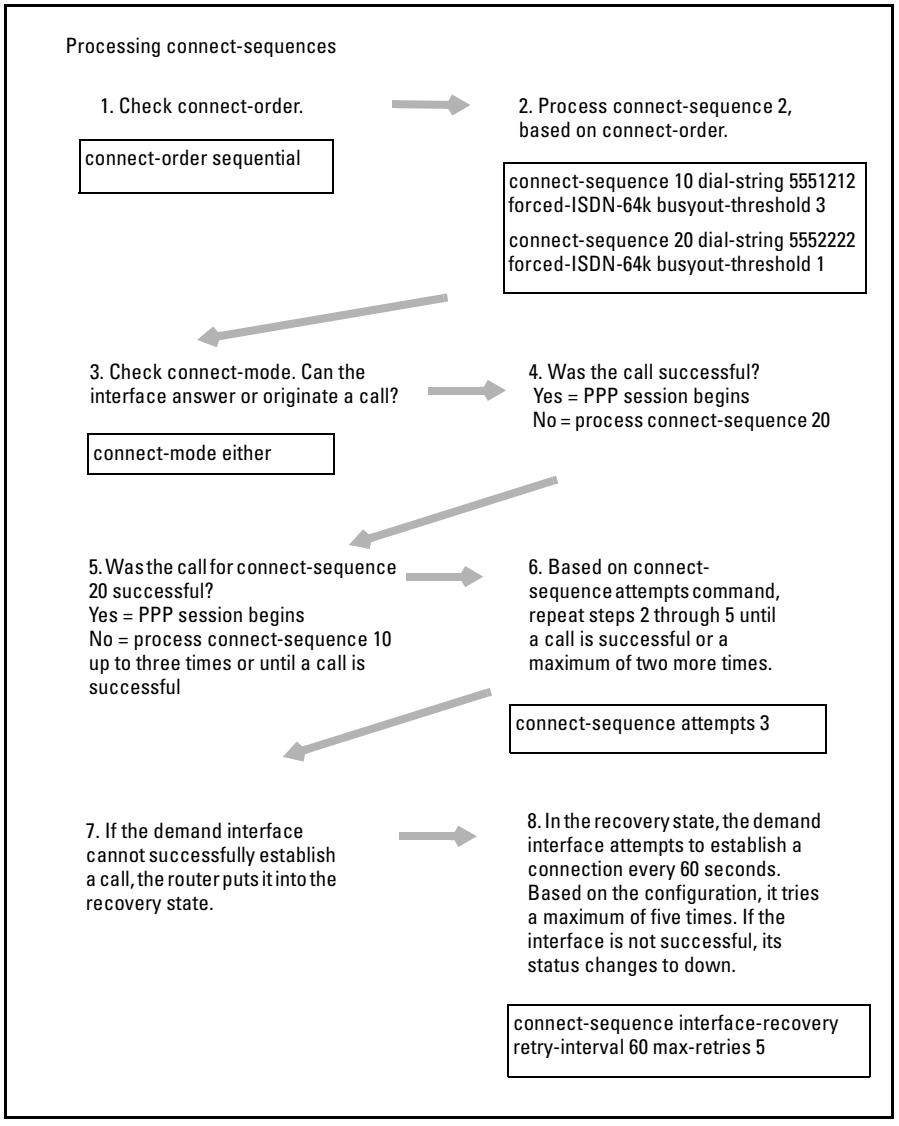

Figure 8-11. Trying to Establish an ISDN Connection

If the ISDN connection is not established, the ProCurve Secure Router will try to process connect sequence 20. Because the **busyout-threshold** setting is **1**, the ProCurve Secure Router will try this connection only once. If the second connect sequence is unsuccessful, the ProCurve Secure Router will try connect sequence 10 up to two more times (for a total of three times).

If the ProCurve Secure Router processes all of the connect sequences and cannot establish a dial-up connection, the connect sequence attempt fails. For the configuration shown in Figure 8-10, the ProCurve Secure Router will cycle through the connect sequences three times. That is, it will attempt to call 5551212 (connect sequence 10) up to nine times in total and 5552222 (connect sequence 20) up to three times in total.

If all three attempts are unsuccessful, the ProCurve Secure Router will change the status of the demand interface to down (recovery active). Further, the router will remove the demand interface's IP address and any routes referencing the interface (allowing any routes with higher administrative distances to take their place).

In 60 seconds, the ProCurve Secure Router will try to process the connect sequences again (although the demand interface will remain in recovery active mode). That is, the router will call 5551212 once, 5552222 once, and then 5551212 twice again. If that attempt is unsuccessful, the ProCurve Secure Router will try again in 60 seconds. Based on the configuration in Figure 8-10, the ProCurve Secure Router will try up to five times or until a connection is successful.

If all the connection attempts made during the recovery active mode are unsuccessful, the ProCurve Secure Router will change the status of the demand interface to down (recovery failed) until you take some action to intervene. (See "Troubleshooting Demand Routing" on page 8-70.) If a connection is successful, the ProCurve Secure Router will change the status of the demand interface to up (connected), activate the IP address for the interface, and reinstate any routes to the interface.

Configuring the idle-timeout Option

You can configure the amount of time that the demand interface remains up in the absence of interesting traffic. From the demand interface configuration mode context, enter:

Syntax: idle-timeout <*seconds*>

Replace ***<seconds>*** with a number between 1 and 2147483. (The range is 1 second to more than 596 hours.)

The default setting is 120 seconds.

Configuring the fast-idle Option

You can assign BRI interfaces to more than one resource pool. For example, you might want to assign backup interfaces to more than one resource pool because it would be unlikely that two primary interfaces would go down at the same time. If at all possible, however, ProCurve Networking recommends that you design resource pools and the connect sequences to avoid contention for BRI interfaces—especially for primary BRI interfaces.

If all the BRI interfaces in a resource pool are in use and the ProCurve Secure Router needs to establish another connection, the **fast-idle** option determines the number of seconds that the existing ISDN connections will remain up in the absence of interesting traffic. Because BRI interfaces are in contention, the **fast-idle** option drastically reduces the time the demand remains up when it is not in use.

To configure this setting, enter the following command from the demand interface configuration mode context:

Syntax: fast-idle <*seconds*>

Replace ***<seconds>*** with a number between 1 and 2147483. (The range is 1 second to more than 596 hours.)

The default setting is 20 seconds.

To return the option to the default setting, enter:

```
ProCurve(config-demand 1)# no fast-idle
```

Defining the caller-number Option

When an ISDN call is established, the calling party supplies a Calling Line ID (CLID). If you configure a **caller-number**, the demand interface will check the CLID when it receives calls. If the CLID matches one of the numbers that you have specified, the demand interface will answer the call. If the number does not match a number, the interface will not answer the call.

You can enter multiple **caller-number** commands, allowing the BRI interface to accept calls from different remote offices or devices.

From the demand interface configuration mode context, enter:

Syntax: caller-number <*CLID*>

Replace ***<CLID>*** with the calling party's telephone number.

By default, the **caller-number** list does not include any numbers so all calls are accepted.

Defining the called-number Option

You can also configure the Dialed Number Identification Service (DNIS) that the demand interface provides when answering a call. From the demand configuration mode context, enter:

Syntax: called-number <*DNIS*>

Replace ***<DNIS>*** with the telephone number that you want the BRI interface to provide when answering or making a call. This command allows the router to provide the same caller ID to a remote peer no matter which physical interface it uses to make the connection.

You can enter multiple **called-number** commands. By default, no number is specified for the **called-number** command.

Configuring the Hold Queue

When the ProCurve Secure Router detects interesting traffic, it begins to hold these packets in a queue while it tries to set up a dial-up connection. When the connection is established, the ProCurve Secure Router transmits all the packets in the hold queue.

You can configure the maximum number of interesting packets that the router keeps in the hold queue and the length of time the packets are held while a connection is being made. From the demand interface configuration mode context, enter:

Syntax: demand-hold-queue <*packets*> timeout <*seconds*>

Replace ***<packets>*** with a number between 0 and 200. Replace ***<seconds>*** with a number between 0 and 255.

By default, the ProCurve Secure Router holds 200 packets for 3 seconds. If the number of packets received before the connection is established exceeds 200 packets or if the connection is not established within 3 seconds, the ProCurve Secure Router empties the hold queue. However, emptying the hold queue does not terminate an activation attempt.

Configuring the BRI Interface

To configure the BRI interface, you need the following information from your service provider:

- ISDN signaling (switch) type
- assigned telephone numbers (LDNs)
- service profile IDs (SPIDs), if you are located in the United States or Canada

You should have this information available before you begin configuring the BRI interface. You must then complete the following steps:

1. Access the BRI interface configuration mode context.
2. Specify the ISDN switch type.
3. Assign the BRI interface a SPID and LDN if you are using a BRI U interface module.
4. Assign the interface an LDN if you are using a BRI S/T interface.
5. Activate the BRI interface.

Accessing the BRI Interface

To access the BRI interface configuration mode context, enter:

Syntax: interface <*interface*> <*slot*>/<*port*>

Replace ***<interface>*** with **bri**.

On the ProCurve Secure Router, each physical interface is identified by its slot number and port number.

The possible slot numbers for a primary ISDN interface are:

- 1 = dl option module slot 1
- 2 = dl option module slot 2

The port number you enter depends on the location of the module you are configuring. Each of the ProCurve ISDN modules has three ports: two ISDN BRI ports (ports 1 and 2) and a backup ISDN BRI port (port 3). For more information about backup ports, see the *Advanced Management and Configuration Guide, Chapter 3: Configuring Backup WAN Connections*.

For example, if the ISDN module is located in slot 1 and you are configuring the interface for port 2, enter.

```
ProCurve(config)# interface bri 1/2
```

The prompt should indicate that you have entered the appropriate interface configuration mode context:

```
ProCurve(config-bri 1/2)#
```

Configuring the ISDN Signaling (Switch) Type

The ProCurve Secure Router ISDN module supports the AT&T 5ESS, Northern DMS-100, Euro NET3, and National ISDN-1 standards. You must configure the BRI interface to use the ISDN signaling that your public carrier uses. The signaling type does not necessarily have to be that of the ISDN switch's manufacturer. For example, a Lucent switch can implement National ISDN-1 signaling. Your public carrier should inform you which signaling method it uses.

To set the signaling type, enter the following command from the BRI interface configuration mode context:

Syntax: isdn switch-type [basic-5ess | basic-dms | basic-net3 | basic-ni]

```
ProCurve(config-bri 1/2)# isdn switch-type basic-5ess
```

Table 8-8 lists the command syntax for specifying each signaling type.

Table 8-8. ISDN Signaling Types

Signaling Type	Command Syntax
National ISDN-1	**isdn switch-type basic-ni**
Euro ISDN	**isdn switch-type basic-net3**
Northern Telecom DMS-100	**isdn switch-type basic-dms**
Lucent/ATT 5ESS	**isdn switch-type basic-5ess**

The default settings are:

- ISDN BRI U modules, **isdn switch-type basic-5ess**
- ISDN BRI S/T modules, **isdn switch-type basic-net3**

If your public carrier is using the default signaling type, you do not have to enter the **isdn switch-type** command. You can simply accept the default setting.

Configuring a SPID and LDN for ISDN BRI U Modules

In North America, some ISDN switches require a SPID to identify each TE on the subscriber's premises and to determine the types of services that the TE can access. A SPID is typically a 14-digit number that includes the interface's 10-digit telephone or local directory number (LDN) and a two- to four-digit identifier. This identifier specifies the type of service on the line (data or voice). If the public carrier's switch requires a SPID, you must specify it when you set up your ISDN equipment.

If you are configuring a router for an ISDN connection in North America, enter the following command to set the SPID:

Syntax: isdn spid1 <*SPID1*>

Some public carriers assign two SPIDs to ISDN connections that use both channels. You must set the second SPID in order for the second B channel to properly receive data. You set the second SPID using the **isdn spid2** command:

Syntax: isdn spid2 <*SPID2*>

You can set a SPID and an LDN in one command. Enter:

Syntax: isdn spid1 <*SPID1*> <*LDN1*>

For example, you might enter:

```
ProCurve(config-bri 1/3)# isdn spid1 70455511110101 5555551111
```

Similarly, you can set a second LDN at the same time that you set the second SPID.

```
ProCurve(config-bri 1/3)# isdn spid2 70455511120101 5555551112
```

Alternatively, you can set an LDN using a separate command.

Syntax: isdn ldn1 <*LDN1*>
Syntax: isdn ldn2 <*LDN2*>

Note

You can set LDNs using the **isdn ldn1**, **isdn ldn2**, **isdn spid1**, or **isdn spid2** commands. The router uses whatever LDN1 or LDN2 value that was most recently entered using one of these commands.

Configuring an LDN for BRI S/T Modules

The LDN is the PTT or PSTN number that the remote peer calls to reach the BRI interface and establish the WAN link. You must set the LDN in order for the interface to answer calls.

Setting the LDN. Enter the LDN with the **isdn ldn1** command:

Syntax: isdn ldn1 <*LDN*>

For example, you might enter:

```
ProCurve(config-bri 1/2)# isdn ldn1 5555551111
```

You can also set a secondary LDN using the **isdn ldn2** command:

```
ProCurve(config-bri 1/1)# isdn ldn2 5555552222
```

If you are configuring an ISDN line that uses SPIDs (typically a North American ISDN line), you can set the SPID at the same time that you set the LDN.

Activating the Interface

The BRI interface must be manually activated. From the BRI interface configuration mode context, enter:

Syntax: no shutdown

Caller ID Options

If you configure the ProCurve Secure Router to accept ISDN calls from certain numbers, the router checks each incoming call's caller ID to ensure it matches your list of acceptable numbers. You can override an incoming call's caller ID using the **caller-id override** option. Enter:

Syntax: caller-id override [always <*number*> | if-no-cid <*number*>]

Replace ***<number>*** with the phone number that you want to use to override the incoming caller id number. The **always** option replaces the caller ID for all incoming calls with the number you specify. The **if-no-cid** option uses the specified number only when an incoming call does not have a caller ID.

Configuring the ISDN Group

When you configure demand routing for a primary ISDN connection, you must configure an ISDN group by completing the following steps:

1. Create an ISDN group.
2. Assign BRI interfaces to the group.
3. Make the ISDN group a member of a resource pool.
4. Configure an **incoming-accept-number**.

Creating an ISDN Group

From the global configuration mode context, enter:

Syntax: isdn-group <*number*>

Replace ***<number>*** with a number between 1 and 255 to uniquely identify this ISDN group.

You are moved to the ISDN group configuration mode context, as shown below:

```
ProCurve(config-isdn-group 1)#
```

From here, you can assign primary BRI interfaces to the group, and you can make this group a member of a resource pool. You can also configure the maximum and minimum number of links for an MLPPP connection. (This is explained in "MLPPP: Increasing Bandwidth" on page 8-50.)

Assigning BRI Interfaces to the ISDN Group

To assign a BRI interface to the ISDN group, enter the following command:

Syntax: connect bri <*slot*>/<*port*>

Replace ***<slot>*** and ***<port>*** with the numbers that identify where the BRI interface is installed. You can assign multiple BRI interfaces to the ISDN group. For example, you might enter:

```
ProCurve(config-isdn-group 1)# connect bri 2/1
ProCurve(config-isdn-group 1)# connect bri 2/2
```

Assigning the ISDN Group to a Resource Pool

To use the ISDN group for demand routing, you must make the group a member of a resource pool. The resource pool must be associated with at least one demand interface.

From the ISDN group configuration mode context, enter:

Syntax: resource pool-member <*poolname*>

For example, if the resource pool is called Branch, enter:

```
ProCurve(config-isdn-group 1)# resource pool-member Branch
```

Note

The ISDN group can be a member of only one resource pool.

Configuring the incoming-accept-number

You can control which calls the BRI interfaces in the ISDN group accept. From the ISDN group configuration mode context, enter:

Syntax: incoming-accept-number <*number*>

Replace **<***number***>** with the number that should be accepted for this ISDN group. The number you enter should match the digits that populate the called party information element (IE) received on the BRI interface answering the call.

You can use the wildcard characters listed in Table 8-9 to specify a range of numbers.

Table 8-9. Wildcard Characters for incoming-accept-number

Wildcard Characters	Explanation
X	Matches any single digit between 0 and 9.
N	Matches any single digit between 2 and 9.
$	Matches any number (multiple numbers). This is the default setting.
[ ]	Matches any digit in the list. For example, if you enter [2,4,6] the ProCurve Secure Router matches only 2, 4, and 6. If you enter [4-6,8] the ProCurve Secure Router matches 4, 5, 6, and 8.

Table 8-10 provide some examples of using wildcard characters.

Table 8-10. Examples of Using Wildcard Characters to Specify incoming-accept-number

Types of incoming-accept-numbers	Pattern
calls for a particular U.S. or Canadian area code	916$
calls for two numbers—such as 555-1111 and 555-1112	555-111[1,2]
calls for a group of numbers—such as the numbers between 555-1000 and 555-2000	555-[1,2]XXX

Using wildcard characters is especially useful if your company uses ISDN hunt groups and all the ISDN interfaces are assigned to the same ISDN group. ISDN hunt groups bundle multiple ISDN interfaces with unique LDNs together into a single group at the public carrier's CO. When the public carrier's CO receives a call to any of the LDNs assigned to the ISDN interfaces in the hunt group, the public carrier's switch sends the call to the first available ISDN interface. The ISDN group, therefore, must be able to accept calls to multiple LDNs. You can use wildcard characters to create a single entry that matches several numbers.

If the number for the BRI interface that is trying to establish a call does not match the **incoming-accept-number**, the call will be rejected.

Configuring a Static Route for the Demand Interface

As explained earlier, the demand interface spoofs an up status, allowing you to create static routes to the far-end network connected through the dial-up interface. To configure a static route to a far-end network, you must enter the following information:

- destination address and subnet mask
- next-hop address or forwarding interface

By default, the administrative distance for a static route is 1 and the metric is 0.

Note

ProCurve Networking recommends that you use static routes for ISDN connections, rather than a dynamic routing protocol. Because routing protocols regularly exchange updates, these updates frequently initiate the ISDN connection, resulting in higher cost for your company's ISDN line. (If you want to send routing updates over the ISDN link, you can configure the ACL that defines interesting traffic so that it does *not* include routing updates. You can then apply an ACL or ACP to the demand interface to allow the routing updates if the ISDN connection is already established. For more information, see "Applying an ACP or Another ACL to the Demand Interface" on page 8-27.)

You can view the type of information the ProCurve Secure Router stores in its routing table by entering the following command from the enable mode context:

ProCurve# show ip route

Figure 8-12 shows the type of information that is displayed.

```
ProCurve# show ip route
C    10.2.2.0/30 is directly connected, ppp 1
C    10.3.3.0/30 is directly connected, demand 1
C    192.168.20.0/24 is directly connected, eth 0/1
S    192.168.30.0/24 [1/0] via 10.2.2.2, ppp 1
S    192.168.7.0/24 [1/0] via 0.0.0.0, demand 1
```

Figure 8-12. Routing Table with Static Routes

To configure a static route, enter the following command from the global configuration mode context:

Syntax: ip route <*destination A.B.C.D*> <*subnet mask* | */prefix length*> <*next hop A.B.C.D* | *forwarding interface ID*>

Replace <*destination A.B.C.D*> with the IP address for the far-end network. For example, the far-end network might be network 192.168.7.0. Next, either specify the complete subnet mask (such as 255.255.255.0) or enter the prefix length (such as /24). Then, specify the forwarding interface as demand ***<number>***. To configure a route to network 192.168.7.0 /24 through demand interface 1, enter:

ProCurve(config)# ip route 192.168.7.0 /24 demand 1

For more information about configuring static routes, see "Static Routing" on page 11-9 of *Chapter 11: IP Routing—Configuring Static Routes*.

After you have configured the static route, you should test your configuration to ensure that the ISDN connection is triggered by the appropriate traffic. (For example, you can use the extended **ping** command to simulate a packet that matches the criteria for interesting traffic.) If the ISDN connection is not established successfully, you should check your configuration. Enter **show running-config** from the enable mode context and look for any obvious configuration errors. If you do not immediately find a problem, see "Troubleshooting Demand Routing" on page 8-70.

Example of a Successful Demand Interface Call

Figure 8-13 shows the successful establishment of an ISDN connection using the demand interface.

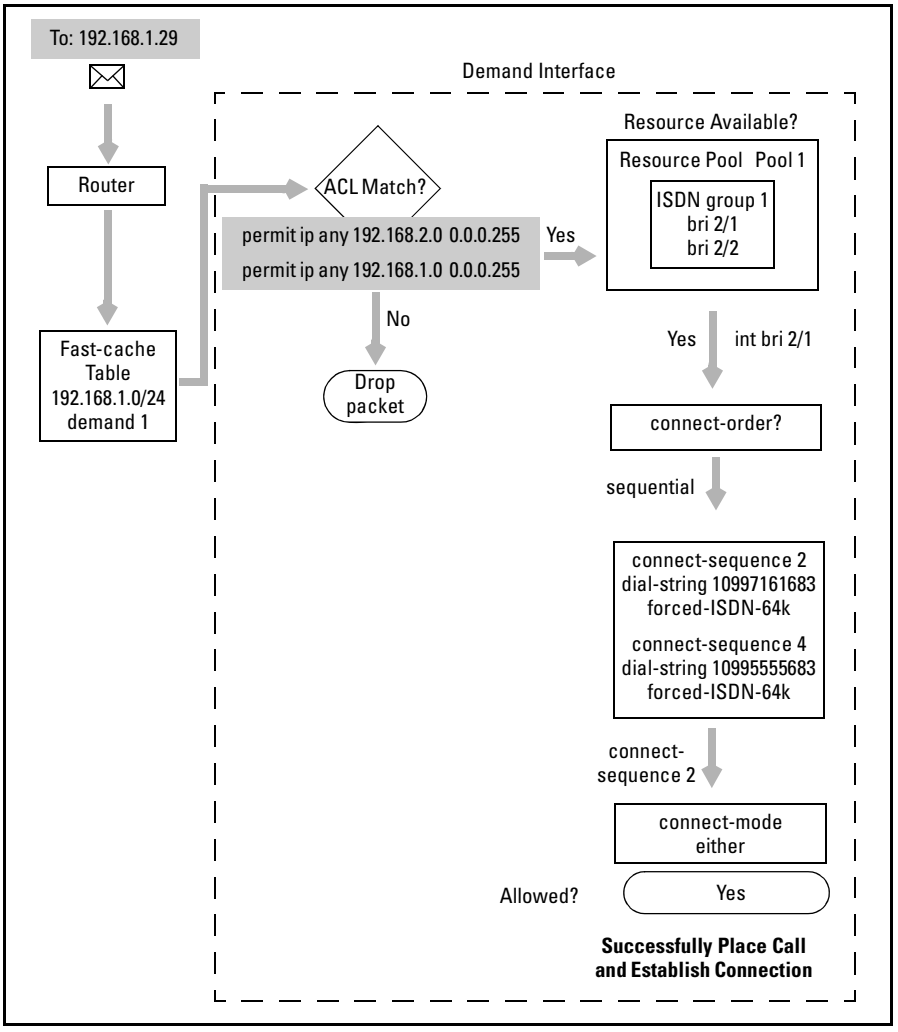

Figure 8-13. Successful Demand Interface Call Setup

When a packet is received on the router, it goes through several processes before it is finally forwarded across a WAN connection. If fast caching is enabled, the router takes a moment to check the fast-cache table. In this example, all traffic to the 192.168.1.0 network has a fast-cache route through the demand 1 interface. The router matches the incoming packet with this route and forwards it to the demand interface. (If the packet did not match an entry in the fast-cache table, the router would match it a route in its standard routing table.)

After the packet has been sent to the demand interface, the router checks the fields in the packet's IP header (such as source and destination address) against the **match-interesting list** ACL. If the packet does not match the list, the router drops it. If the packet does match, the demand interface checks its resource pools.

The demand interface searches for the first available interface in its resource pool. In this example, the first resource in resource pool Pool1 is ISDN group 1. Within the ISDN group, the first interface is BRI 2/1. If the BRI 2/1 interface is available, the demand interface begins checking its connect sequences for one that matches with the BRI interface resource.

If a connect sequence is found that permits the demand interface to use the BRI resource interface, the demand interface next checks the connect mode configuration.

If the connect mode is set to the **originate** or **either** options, the demand interface places a call through the BRI resource interface. If the call connects, the demand interface can then forward the packet through the BRI interface toward its destination.

MLPPP: Increasing Bandwidth

If you are configuring demand routing for a primary BRI interface, you can aggregate multiple B channels to increase bandwidth. Specifically, you use multilink PPP (MLPPP) to aggregate the multiple channels. To configure MLPPP for BRI interfaces, you must:

1. Enable MLPPP for incoming calls.
2. Enable MLPPP for the demand interface that is managing the BRI interfaces that you want to aggregate.
3. Configure the minimum and maximum channels for the ISDN group.

Configuring MLPPP for Incoming Calls

To enable the negotiation of MLPPP for incoming calls, enter the following command from the global configuration mode context:

```
ProCurve(config)# data-call multilink
```

To disable MLPPP for incoming calls, enter:

```
ProCurve(config)# no data-call multilink
```

By default, MLPPP is disabled for incoming calls.

Configuring MLPPP for Demand Interfaces

To enable MLPPP, enter the following command from the demand interface configuration mode context:

```
ProCurve(config-demand 1)# ppp multilink
```

By default, MLPPP is not enabled.

Configuring the Maximum Number of Interfaces. You can configure the maximum number of interfaces that the demand interface can aggregate for an MLPPP connection. From the demand interface configuration mode context, enter:

Syntax: ppp multilink maximum <*interfaces*>

Replace ***<interfaces>*** with a number between 1 and 8. If MLPPP is enabled for the demand interface, the default value for the maximum number of interfaces is 8.

Note

The **ppp multilink maximum** command does not affect the number of links used when an interface *answers* a call, only when it originates a call.

Configuring the MLPPP Interleave. If you configure quality of service (QoS) for the dial-up connections established through the demand interface, you may also want to enable MLPPP interleave. Certain types of high-priority packets may be adversely affected if they are transmitted over an MLPPP connection. If interleave is enabled, the demand interface handles high-priority packets differently. When the demand interface receives a high-priority packet, it encapsulates the packet as PPP (rather than MLPPP) and sends it on the next available link.

To enable MLPPP interleave, enter:

```
ProCurve(config-demand 1)# ppp multilink interleave
```

Note

If the MTU for the demand interface is lower than the size of the high-priority packet, the demand interface will drop the packet.

Configuring MLPPP Fragmentation. When a packet is to be transmitted across an MLPPP connection, the demand interface divides the packet into fragments of equal length. If possible, the number of fragments equals the number of active links in the MLPPP and are transmitted simultaneously over each link. Fragmentation may also be controlled by the MTU setting of the demand routing interface.

To enable fragmentation for MLPPP, enter the following command from the demand interface configuration mode context:

```
ProCurve(config-demand 1)# ppp multilink fragmentation
```

Configuring the Minimum and Maximum Channels. When you configure MLPPP for primary BRI interfaces, you must configure the minimum and maximum number of B channels that can be aggregated into a single MLPPP connection. Aggregated channels belong to BRI interfaces that are in the same ISDN group, so you specify the minimum and maximum numbers from an ISDN group configuration mode context. Enter:

Syntax: min-channels <*number*>
Syntax: max-channels <*number*>

Although the range for <***number***> is between 1 and 255, the actual number of channels you can enter is limited by the number of BRI interfaces assigned to the ISDN group. For example, if the ISDN group includes two BRI interfaces, the highest number of channels that can be used is 4 (two channels from each interface).

Example of MLPPP with Demand Routing

Figure 8-14 shows an example configuration of MLPPP configured for a demand interface.

```
interface bri 2/1
  isdn ldn1 968483940096
  no shutdown
!
interface bri 2/2
  isdn ldn1 978484540055
  no shutdown
!
interface demand 1
  idle-timeout 240
  resource pool Pool
  match-interesting list Call out
  match-interesting reverse list Call in
  connect-sequence 1 dial-string 9633333 forced-isdn-64k busyout-threshold 3
  connect-sequence 2 dial-string 9634444 forced-isdn-64k busyout-threshold 3
  connect-sequence interface-recovery retry-interval 120 max-retries 0
  ip address  10.1.1.1  255.255.255.0
  ppp multilink                                    MLPPP enabled
  ppp multilink maximum 2
  no shutdown                          channels
!
isdn-group 1
  min-channels 4
  max-channels 4
  resource pool-member Pool
  connect bri 2/1
  connect bri 2/2
!
ip access-list extended Call
  permit ip any  192.168.2.0 0.0.0.255
!
ip route 192.168.2.0 255.255.255.0 demand 1
```

Figure 8-14. MLPPP Configuration for Demand Routing

Configuring PPP Authentication for an ISDN Connection

If you want to ensure that only authorized peers establish a PPP connection with the demand interfaces on the ProCurve Secure Router, you can configure PPP authentication. The ProCurve Secure Router supports Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) for PPP authentication.

Note

To protect your WAN, ProCurve Networking strongly recommends that you enable PPP authentication for the ISDN connection.

Enabling PPP Authentication for All Demand Interfaces

You must configure the PPP authentication protocol that the router uses for inbound calls. To configure the authentication protocol that the demand interfaces expect to receive for inbound calls, enter the following command from the global configuration mode context:

Syntax: data-call authentication protocol [chap | pap]

Include either the **chap** option or the **pap** option, depending on which PPP authentication protocol you want to use to authenticate peers.

You should also specify which authentication protocol the demand interfaces send to authenticate themselves to a peer when answering a call. From the global configuration mode context, enter:

```
ProCurve(config)# data-call sent authentication protocol [chap | pap]
```

By default no authentication protocol is specified for demand interfaces.

Disabling the Authentication Protocol. To disable the global setting for the PPP authentication protocol that is used for demand routing interfaces, enter:

```
ProCurve(config)# no data-call authentication protocol
ProCurve(config)# no data-call sent authentication protocol
```

Configuring PAP Authentication for a Demand Interface

If you want to use PAP as the authentication protocol, you must configure the username and password that the ProCurve Secure Router sends when the far-end router requests authentication information from a demand interface. From the demand interface configuration mode context, enter:

Syntax: ppp pap sent-username <*username*> password <*password*>

Configuring CHAP Authentication for a Demand Interface

If you want to use CHAP, you must configure the password that the ProCurve Secure Router sends when the far-end router requests authentication information from a demand interface. From the demand interface configuration mode context, enter:

Syntax: ppp chap password <*password*>

When you replace <***password***>, ensure that you are using the same settings that are configured on the far-end router.

The username that is sent is the hostname of the router. If necessary, you can override this username with this demand interface configuration command:

Syntax: ppp chap hostname <*hostname*>

Configuring the Username and Password That the Router Expects to Receive

You must also configure the username and password that the ProCurve Secure Router expects to receive from the far-end router. From the demand interface configuration mode context, enter:

Syntax: username <*username*> password <*password*>

For example, you might enter:

```
ProCurve(config-demand 1)# username SiteB password procurve
```

For CHAP, the username should be the hostname of the peer.

Configuring Peer IP Address

You can also configure the IP address of the PPP peer for the dial-up WAN connection. From the demand interface configuration mode context, enter:

Syntax: peer default ip address <*A.B.C.D*>

Replace ***<A.B.C.D>*** with the IP address of the far-end router.

Example of Demand Routing with PAP Authentication

Figure 8-15 shows a demand routing configuration that uses PAP authentication. The **data-call** commands enable PAP authentication for all demand interfaces configured on the router. The **ppp authentication pap** command enables PAP for the demand interface. The **username** command establishes the username and password that the PPP peer will submit to the ProCurve Secure Router. The **ppp pap sent** command configures the username and password that the ProCurve Secure Router will send its peer.

```
data-call authentication protocol pap
data-call sent authentication protocol pap
!
interface bri 2/1
  isdn ldn1 968483940096
  no shutdown
!
interface bri 2/2
  isdn ldn1 978484540055
  no shutdown
!
interface demand 1
  idle-timeout 240
  resource pool Pool
  match-interesting list Call out
  match-interesting reverse list Call in
  connect-sequence 1 dial-string 9633333 forced-isdn-64k busyout-threshold 3
  connect-sequence 2 dial-string 9634444 forced-isdn-64k busyout-threshold 3
  connect-sequence interface-recovery retry-interval 120 max-retries 0
  ip address  10.1.1.1  255.255.255.0
  ppp authentication pap
  ppp multilink
  ppp multilink maximum 2
  username procurve password procurve
  ppp pap sent-username procurve password procurve
  no shutdown
!
!
isdn-group 1
  min-channels 4
  max-channels 4
  resource pool-member Pool
  connect bri 2/1
  connect bri 2/2
!
ip access-list extended Call
  permit ip any  192.168.2.0 0.0.0.255
!
ip route 192.168.2.0 255.255.255.0 demand 1
```

data-call commands to enable PAP authentication

PAP configured for this demand interface

username and password that the demand interface expects to receive from its PPP peer

username and password that the demand interface sends to its PPP peer

Figure 8-15. Using PAP Authentication with Demand Routing

Setting the MTU for Demand Interfaces

When establishing a link, PPP peers must agree on how much data can be contained in the information field of PPP frames. The value that communicates this frame size is called the maximum receive unit (MRU). To increase or decrease the value of the MRU, a PPP peer sets the MRU configuration option in the Link Control Protocol (LCP). (LCP is one of the protocols in the PPP suite. LCP is used to establish and control the PPP connection.)

To control the MRU that is negotiated between the two PPP peers, you configure the maximum transmission unit (MTU), which defines the largest size for a frame that the router can send over the connection. By default, demand interfaces (which use PPP) have an MTU of 1500 bytes. If a frame exceeds the MTU, it must be fragmented.

To successfully negotiate a PPP session, the two peers should be using the same MTU.

To configure the MTU for all PPP connections used with demand routing, enter:

ProCurve(config)# data-call mtu <*number*>

Replace ***<number>*** with a value between 64 and 1520.

To disable this setting for interfaces used with demand routing, enter:

ProCurve(config)# no data-call mtu

Configuring an ISDN Template

Some companies may want to use an ISDN template to encode the **caller-number** and **called-number** for inbound and outbound calls. This template allows you to configure the prefix and call type globally.

Note

Entering this command is optional; an ISDN template is not required for demand routing.

To create an ISDN template, enter the following command from the global configuration mode context:

Syntax: isdn-number-template <*template id*> prefix <*prefix*> [abbreviated | international | national | network-specific | subscriber | unknown} <*pattern*>

Replace ***<template id>*** with a number between 1 and 255.

Replace ***<prefix>*** with the expected prefix for the call type. If you do not want to specify a prefix, leave this option blank by entering double quotation marks (“”). Do not enter a space between the quotation marks. If you want to specify a prefix, you can enter unlimited-length strings of 0s and 1s. For example, for international calls made from within the United States, you might enter a prefix of **011**.

Specify a call type by entering one of the options listed in Table 8-11.

Table 8-11. Options for Call Type

Call Type	Explanation
abbreviated	Specifies abbreviated (bits 110) in the Type of Number octet. This option is used primarily for private ISDN network applications, and the implementation is network-dependent.
international	Specifies international (bits 001) in the Type of Number octet. This option is used for calls destined outside the national calling area.
national	Specifies national (bits 010) in the Type of Number octet. This option is used for calls inside the national calling area. That is, the calls do not cross an international local access and transport area (LATA).
network-specific	Specifies network-specific (bits 011) in the Type of Number octet. This option is used for calls that require special access to a private network. Because the prefix that must be stripped off once access to the network has been gained, the dialing prefix is removed.
subscriber	Specifies Subscriber (bits 100) in the Type of Number octet. This option is used for intra-LATA calls (local calls). By default, the area code is removed for these calls.
unknown	Specifies Unknown (bits 000) in the Type of Number octet. This option is used if the actual types of the number are not known. Unknown numbers are assumed to have no prefix, and the entire dialed number is used.

Use the options in Table 8-12 to specify a ***<pattern>*** for the call type.

Table 8-12. Characters for Call Patterns

Valid Characters	Explanation
0-9	Match exact digit only.
X	Match any single digit between 0 and 9.
N	Match any single digit between 2 and 9.
M	Match any single digit between 1 and 8.
$	Match any number.
[ ]	Match any digit in the list. For example, if you enter [1,4,6] the ProCurve Secure Router matches only 1, 4, and 6. If you enter [1-3,5] the ProCurve Secure Router matches 1, 2, 3, and 5.

For example, if you want to create a pattern for U.S. local calls, you would enter NXX-XXXX. The N wildcard specifies that the first number can be between 2 and 9. Each X can be any number between 0 and 9.

Other examples of using wildcard characters are listed in Table 8-13.

Table 8-13. Using Characters for Call Pattern

Incoming Numbers That Should Be Accepted	Pattern
calls from one U.S. or Canadian area to another	NXX-NXX-XXXX
calls from one country to another	N$
calls for a particular U.S. or Canadian area code	916$
calls for two numbers—such as 555-1111 and 555-1112	555-111[1,2]
calls for a group of numbers—such as the numbers between 555-1000 and 555-2000	555-[1,2]XXX

Using Call Types and Patterns

Call types and patterns are interdependent, as explained below:

International. If you specify the international call type, the prefix is removed. For example, an international call from within the United States consists of 011-N$. The international prefix is 011, and N$ represents the digits necessary for routing the call at the destination. You would enter:

```
ProCurve(config)# isdn-number-template 1 prefix 011 international N$
```

When the called party information element (IE) is created for this call, the router removes the prefix and places the N$ digits in the Number Digits field.

National. For national calls, the dialing prefix is removed. For example, a call from one U.S. LATA to another uses the format 1-NXX-NXX-XXXX. The U.S. prefix is 1, and NXX-NXX-XXXX represents the 10-digit number necessary for routing the call. When the router creates the called party IE for this call, it removes the prefix and places the NXX-NXX-XXXX digits in the Number Digits field.

Network-Specific. If you specify the network-specific call type, the ProCurve Secure Router removes the prefix for the call when it prepares the called party IE. For example, if the router is making a call to 700-N$, the dialing prefix is 700 and N$ represents the digits necessary for routing the call at the destination. The ProCurve Secure Router removes the prefix and places the N$ in the Number Digits field.

Subscriber. The ProCurve Secure Router also removes the prefix if you specify the subscriber call. For example, if the router is making a call to 916-555-1212, it would remove the 916 prefix and place 555-1212 in the Number Digits field. For areas with mandatory 10-digit dialing, you should enter a blank prefix to ensure that all ten digits are passed to the Number Digits field.

Default ISDN Template

By default, there is one **isdn-number-template** entry:

```
isdn-number-template 0 prefix "" subscriber 911
```

This entry allows you to make emergency calls within the United States.

Viewing Information about Demand Routing

You can use **show** commands to view different aspects of your demand routing configuration. For example, you can view the status of a demand interface and any dial-up connections that are established through a demand interface. Table 8-14 lists the **show** commands for demand routing.

Table 8-14. show Commands for Demand Routing

Command	Description
show interface demand <number>	displays the status of the demand interface
show demand interface demand <number>	displays a summary of information about the demand interface, including the timers, state, physical interface in use (if connection is up), last outgoing call, and last incoming call
show interface <dial-up interface> <slot>/<port>	displays status of physical interface
show demand sessions	displays information about existing dial-up connections established through demand routing
show demand resource pool <pool name>	lists the resources assigned to the resource pool and the demand interface associated with the resource pool
show running-config	displays the current configuration
show running-config interface demand <number>	displays the current configuration for a demand interface

Viewing the Status of the Demand Interface

To view the status of the demand interface, enter the following command from the enable mode context:

Syntax: show interfaces demand <*number*>

For example, to view the status of demand interface 1, enter:

ProCurve# show interfaces demand 1

Figure 8-16 shows the results of this command if demand interface 1 is spoofing its up status and a dial-up connection has not been established. In addition to showing the status of the interface, this command displays settings for the following commands:

- **connect-mode**
- **resource pool**
- **connect-sequence**
- **idle-timeout**
- **fast-idle**
- **ip address**

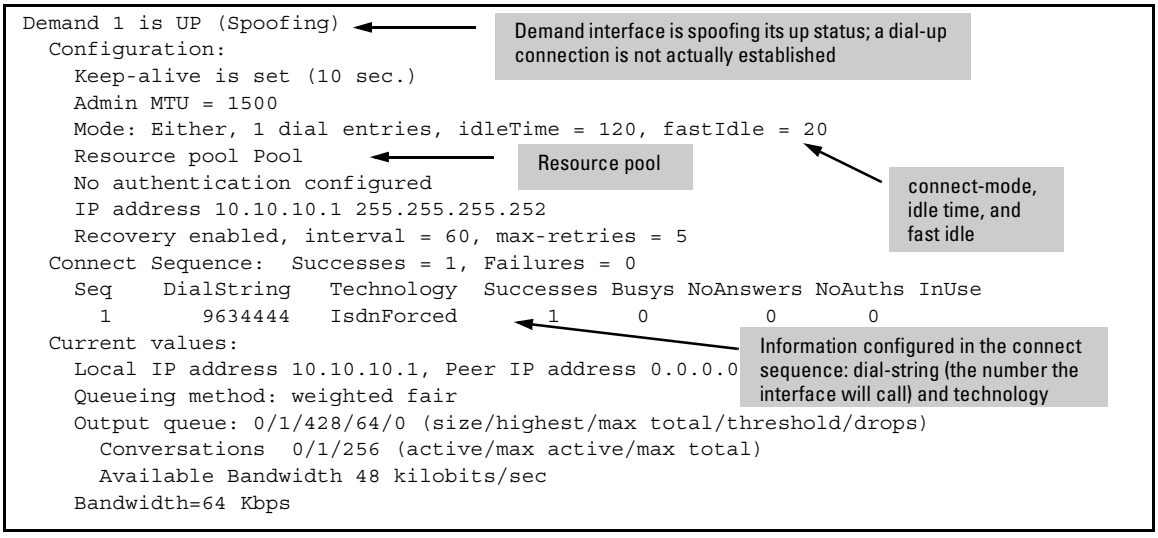

Figure 8-16. Viewing the Status of the Demand Interface When a Dial-Up Connection Has Not Been Established

If a connection has been established through the demand interface, the **show interfaces demand 1** command shows:

- the number of seconds until the ISDN connection is terminated
- the number of frames in and out
- the traffic that triggered the connection (the interesting traffic)
- the amount of time the connection has been up
- the BRI interface and channel through which the connection was established

Figure 8-17 provides the results of the **show interfaces demand 1** command when an ISDN connection has been established.

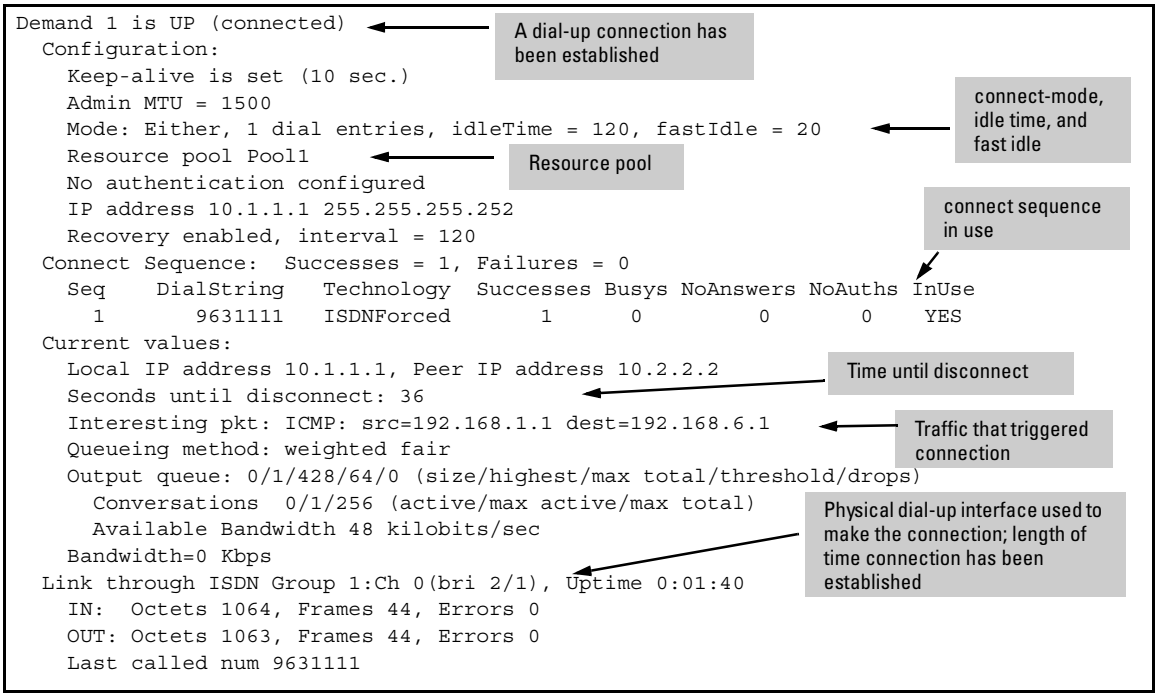

Figure 8-17. Viewing the Status of the Demand Interface When an ISDN Connection Is Established

Viewing a Summary of Information about the Demand Interface

To view a summary of information about the demand interface, enter:

Syntax: show demand interfaces demand <*number*>

This command displays:

- settings for the **idle-timeout** and **fast-idle**
- state of the dial-up connection
- traffic that triggered the dial-up connection
- time until disconnect
- last incoming and outgoing call

As Figure 8-18 shows, this command also lists multiple channels if MLPPP is configured for the ISDN connection.

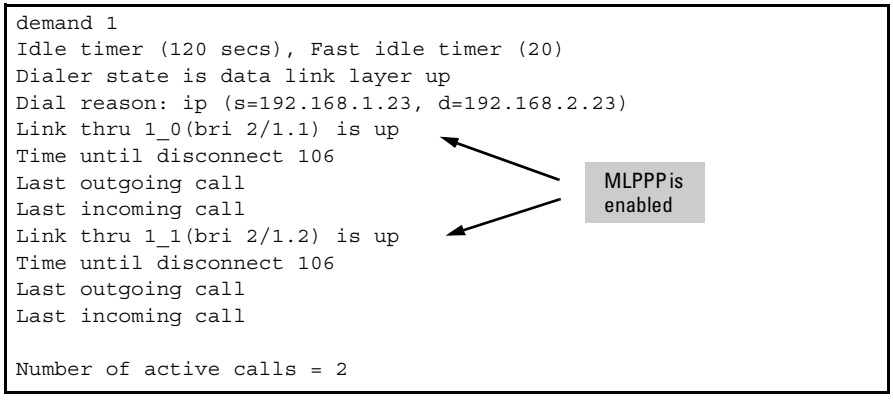

Figure 8-18. Summary Information for Demand 1 Interface

Viewing Settings Configured for the ISDN Group

You can view both the default and the configured settings for a particular ISDN group. From the enable mode context, enter:

Syntax: show isdn-group <number>

Replace ***<number>*** with the number of the group for which you want to view information. For example, to view the settings for ISDN group 2, enter the following command from the enable mode context:

ProCurve# show isdn-group 2

Figure 8-19 shows the settings for an example ISDN group.

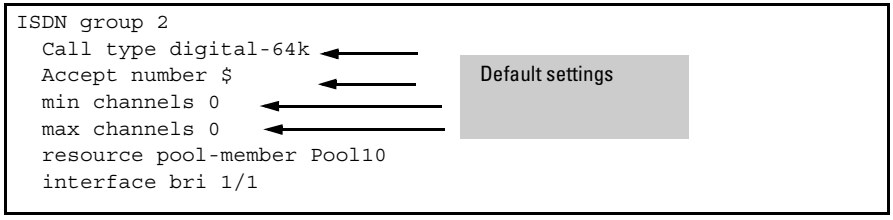

Figure 8-19. Viewing Settings for an ISDN Group

Note

If you do not enter a value for **min channels** and **max channels** and you enter the **show isdn-group** command, these options are displayed with the value set to **0**. At this value, the options are disabled.

Viewing the Status of the BRI Interface

To view the status of a BRI interface that is associated with the demand interface, enter:

Syntax: show interface bri <*slot*>/<*port*>

Replace ***<slot>*** with the slot number in which the backup module is installed, and replace ***<port>*** with the appropriate port number.

For example, to view the status of the BRI 2/1 interface, enter:

```
ProCurve# show interface bri 2/1
```

This command reports the status of the BRI interface and the status of the line. The status of the BRI interface should always be up, indicating that it is either available to make a connection or it is already maintaining a connection. If the BRI interface is down, you must bring it up, or it will not be able to place or receive any calls.

The line status indicates whether or not the BRI interface has established a connection. If the interface has not established a connection, the line status should be “ready,” as shown in Figure 8-20.

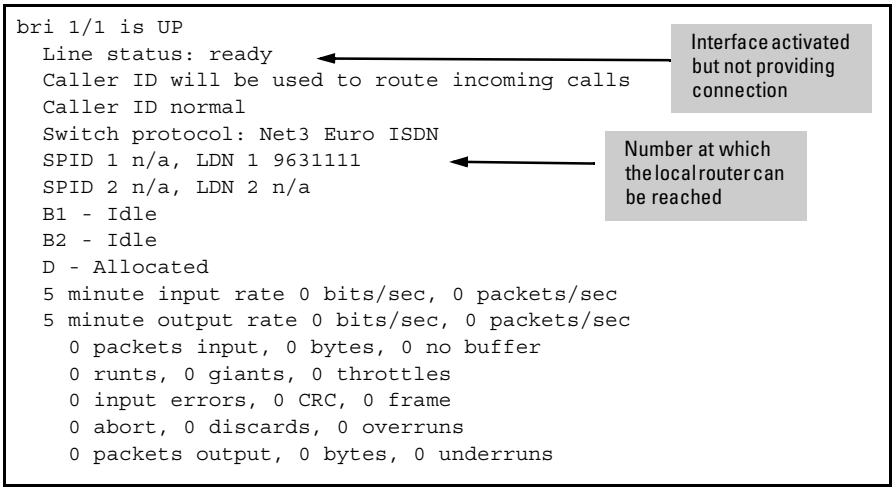

Figure 8-20. Viewing the Status of a BRI Interface

In addition to displaying status information, the **show interfaces bri** command lists settings such as the ISDN switch signaling type, LDN, and SPID (if a SPID is configured) so you can use this command to verify that these settings are configured correctly.

If your public carrier requires a SPID, double-check to see if you were assigned one or two SPIDs. When you use both B channels, public carriers using National ISDN and Northern Telecom DMS-100 switching sometimes require you to configure a SPID for each channel.

Figure 8-21 shows the results of entering the **show interfaces bri** command for a BRI interface that is in use. If the BRI interface is in use, you can view packet statistics and errors for the ISDN connection. (For information about other line status settings, see “Checking the Demand Interface” on page 8-70.)

```
bri 1/2 is UP
  Line status: connected
  Caller ID will be used to route incoming calls
  Caller ID normal
  Switch protocol: Net3 Euro ISDN
  SPID 1 n/a, LDN 1 9631111
  SPID 2 n/a, LDN 2 n/a
  5 minute input rate 112 bits/sec, 0 packets/sec
  5 minute output rate 112 bits/sec, 0 packets/sec
    155 packets input, 8467 bytes, 0 no buffer
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame
    0 abort, 0 discards, 0 overruns
    157 packets output, 8408 bytes, 0 underruns
```

Figure 8-21. Viewing the Status of a BRI Interface That Is in Use

Viewing Demand Sessions

You can view all of the dial-up connections currently established through demand routing. From the enable mode context, enter:

```
ProCurve# show demand sessions
```

The sessions are listed in the order in which they were established. (See Figure 8-22.) For each session, this command lists:

- demand interface through which the connection was established
- IP address of the demand interface and the far-end router
- interesting traffic that triggered the connection
- number of links for each session if MLPPP is enabled
- BRI interfaces through which the links were established
- connection time
- **idle-timeout** setting

```
Session 1
Interface demand 1
Local IP address = 10.1.1.1
Remote IP address = 10.2.2.1
Remote Username =
Dial reason: ip (s=192.168.1.23, d=192.168.2.23)
Link 1
  Dialed number =
  Resource interface = 1_0(bri 2/1.1), Multilink
  Connect time: 0:1:28
  Idle Timer: 120
Link 1
  Dialed number =
  Resource interface = 1_1(bri 2/1.2), Multilink
  Connect time: 0:1:28
  Idle Timer: 120
```

Connection is through channel 1 and channel 2 on the BRI 2/1 interface (bri 2/1.1 and bri 2/1.2)

Figure 8-22. Viewing Demand Sessions

Viewing the Resource Pool

You can view which interfaces or ISDN groups have been assigned to a particular resource pool. You can also view which demand interfaces use the pool. (See Figure 8-23.) From the enable mode context, enter:

ProCurve# show demand resource pool <*poolname*>

```
Pool backup
          Resources:             1_0, 1_1, bri 1/3
          Demand Interfaces:     demand 1
```

Figure 8-23. Viewing a Resource Pool

Show the Running-Config for the Demand Interface

To check your demand routing configuration, you must view the entire running-config file. From the enable mode context, enter:

ProCurve# show running-config

You must then scroll through the file to find the various commands you entered for demand routing.

To view the configuration of just the demand interface, enter:

ProCurve# show running-config interface demand <*number*>

Figure 8-24 shows the running-config for a demand interface that is configured to use MLPPP and PPP authentication.

```
interface demand 1
  idle-timeout 240
  resource pool Pool
  match-interesting list Call out
  match-interesting reverse list Call in
  connect-sequence 1 dial-string 9633333 forced-isdn-64k busyout-threshold 3
  connect-sequence 2 dial-string 9634444 forced-isdn-64k busyout-threshold 3
  connect-sequence interface-recovery retry-interval 120 max-retries 0
  ip address  10.1.1.1  255.255.255.0
  ppp authentication pap
  ppp multilink
  ppp multilink maximum 2
  username procurve password procurve
  ppp pap sent-username procurve password procurve
  no shutdown
```

Figure 8-24. Viewing the Running-Config for a Demand Interface

Troubleshooting Demand Routing

After you configure demand routing, you should test your configuration to ensure that it is working correctly. Is the right traffic triggering the connection, and can the BRI interface successfully establish a connection to the far-end router? Are your settings for the **idle-timeout** and the **fast-idle** sufficient for your WAN environment?

Checking the Demand Interface

The first step you should take to check your configuration is also the first step you should take to troubleshoot demand routing. You should ensure that the demand interface and its associated BRI interfaces are ready to make a connection.

Use the **show interfaces demand** command to view the status of the demand interface, which should be up (spoofing). If the demand interface is down, ensure that you have assigned it a valid IP address. If you configured the demand interface as an unnumbered interface, make sure that the interface with the actual IP address is up.

If the demand interface went down because it could not establish a connection during the recovery mode, its status will be down (recovery failed). In this case, you must identify the problem causing the failure and then you must clear the connection so that the status of the demand interface returns to up (spoofing). Until then, the demand interface cannot establish an ISDN connection.

To clear the ISDN connection, shut down the demand interface. From the demand interface configuration mode context, enter:

```
ProCurve(config-demand 1)# shutdown
```

To re-activate the interface, enter:

```
ProCurve(config-demand 1)# no shutdown
```

Checking the BRI Interface

To ensure that the status of the BRI interface is up and the line status is ready, enter the following command from the enable mode context:

ProCurve# show interface bri <*slot*>/<*number*>

If the BRI interface is administratively down, enter **no shutdown** to activate it.

When you activate the BRI interface, it exchanges a series of messages with the ISDN switch at the CO. First, the BRI interface and the switch complete a handshaking process to bring up the Physical Layer. Then the ISDN switch polls the line for terminal equipment identifiers (TEIs), which identify the ISDN line.

The TEI #1 identifies the first B channel, and the TEI #2 identifies the second. The BRI interface sends the LDNs and/or SPIDs configured for the channels (SPID1 for the TEI #1 and SPID2 for the TEI #2). After the switch receives the correct SPIDs or LDNs, the ISDN line goes up.

When you enter the **show interfaces bri** command, the line status indicates the point at which the handshaking process breaks down. For example, in Figure 8-25 the ISDN switch is attempting to get the BRI interface's SPID1.

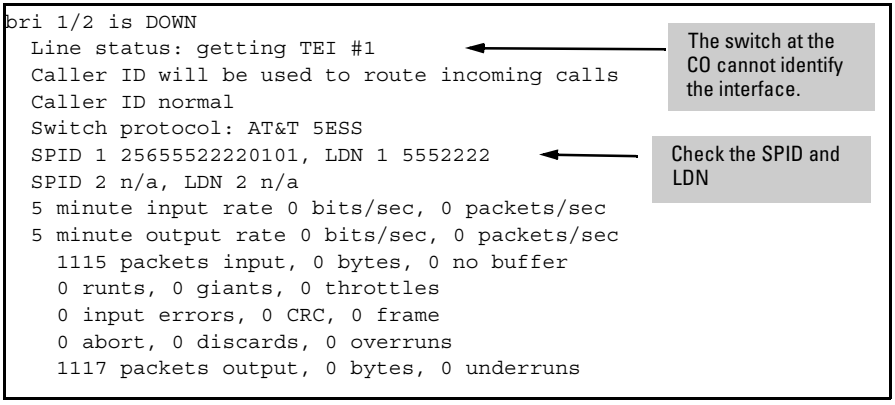

Figure 8-25. Troubleshooting a BRI Interface

Table 8-15 lists the possible designations for the line status and the steps you might take to change the status.

Table 8-15. BRI Line Status

Status	Meaning	Next Best Step
disconnected	The interface is up but has disconnected from the peer. Settings on the demand interface may be preventing the call from connecting. For example, the peer's caller ID does not match number specified with the **calling-number** command.	This status may indicate that an unauthorized peer tried to connect to your router. If the peer is authorized, however, check the settings on the BRI interface or demand interface and change them as needed to allow the connection. Also, check the configuration on the peer to ensure that its settings allow a connection to this BRI interface.
deactivated	The interface may be up or down. The CO has deactivated the interface. The BRI interface may be in the process of communicating with the switch at the CO.	Check with your service provider.
layer 1 down	There is no activity on the ISDN line.	Check the physical hardware, including the cabling and wall jack.
getting TEI #1	The switch cannot identify the BRI interface.	• Check for a miskeyed SPID1 and/or LDN. • Verify that the **isdn switch-type** setting matches the public carrier's signaling type.
getting TEI #2	The switch cannot identify the BRI interface (second B channel).	• Check for a miskeyed SPID2 and/or LDN. • If you should not have to enter a second SPID, the interface may be configured for the wrong signaling type.
TEI #2 OK Getting SPID #2	The switch is having trouble bringing the interface up.	• Try resetting the connection. You may need to reload the router, if possible.

Miskeyed SPIDs and LDNs are the most common problems. Try reentering the SPID and, if necessary, reloading the router so that the BRI interface will be forced to re-initiate the handshaking process. Or enter **maintenance reset** to reset the port hardware.

Remember, however, that the wrong configuration for the switch-type can also cause the status to remain at "getting TE1 #1" or "getting TE1 #2." The switch-type depends on the type of ISDN signaling the public carrier institutes on the line, which depends on its software, not necessarily on the switch's manufacturer.

Checking the ACL That Defines the Interesting Traffic

If the demand interface is up, you should ensure that the interesting traffic actually triggers the ISDN connection. Check the routing table to ensure that the demand interface is listed as a directly connected interface and that the route you entered for the far-end network lists the demand interface as the forwarding interface. From the enable mode context, enter:

```
ProCurve# show ip route
```

If the route is correct, you can send some traffic to the far-end network to determine if the ACL is triggering ISDN traffic. Even a simple **ping** command should start the demand routing process (as long as the ping matches the ACL—for example, you may need to use the extended **ping** commands to set the source address for the ping to a local network address). Before you send the sample traffic, enable debugging for demand routing. From the enable mode context, enter:

```
ProCurve# debug demand-routing
```

If you have configured your ACL correctly, debug messages for demand routing should appear immediately. If no messages appear, you may have configured the ACL incorrectly. Double-check the permit statement you configured, and ensure that you applied the ACL to the demand interface. To check this information, enter the **show running-config** command from the enable mode context.

If you can troubleshoot the problem after business hours (when you will not inadvertently interrupt the flow of traffic to other interfaces), you may want to change the ACL to select all traffic from any source to any destination. The ACL should then trigger the ISDN connection. You can then begin to narrow the scope of the ACL to limit the traffic selected.

Troubleshooting the ISDN Connection

If the interesting traffic triggers the ISDN connection, the ProCurve Secure Router will find the appropriate **connect-sequence** command to process (based on your configuration) and try to establish a connection. If the router is unable to establish this connection, you will need to monitor the call setup.

The Secure Router OS provides a number of ISDN **debug** commands, which are listed in Table 8-16.

Table 8-16. debug Commands for ISDN

Command	Description
debug isdn cc-ie	displays information about the ISDN call control
debug isdn cc-messages	displays call control messages
debug isdn endpoint	displays events related to ISDN endpoints
debug isdn events	displays information about ISDN events
debug isdn group	display errors and messages related to ISDN groups
debug isdn interface	displays ISDN interface events
debug isdn l2-formatted	displays Layer 2 formatted messages
debug isdn l2-messages	displays Layer 2 message
debug isdn resource-manager	displays resource manager errors and messages
debug isdn verbose	display all errors and messages

Note

Debug functions are processor intensive. The debug isdn commands in particular display a high volume of messages to the CLI.

Some of the **debug isdn** commands display numerous messages, which are displayed too quickly to read. You will probably need to stop the messages and review them to determine the problem. For example, Figure 8-26 shows a small portion of the debug messages displayed as a call connects.

```
2005.10.08 11:23:09 L2_MSG BRI 2/1 Recd  = 02 FF 03 08 01 01 05 A1 04 02 88 90 18 01 89 6C
2005.10.08 11:23:09 L2_MSG BRI 2/1         0C 21 80 30 30 30 39 36 33 31 31 31 31 70 08 C1
2005.10.08 11:23:09 L2_MSG BRI 2/1          39 36 33 33 33 33 33
2005.10.08 11:23:09 L2_FMT BRI 2/1 ==========================================
2005.10.08 11:23:09 L2_FMT BRI 2/1 Recd = Sapi:00  C/R:C Tei:7F
2005.10.08 11:23:09 L2_FMT BRI 2/1        Ctl:UI
2005.10.08 11:23:09 L2_FMT BRI 2/1        Prot:08  CRL:1  CRV:0001
2005.10.08 11:23:09 L2_FMT BRI 2/1        M - 05 SETUP
2005.10.08 11:23:09 L2_FMT BRI 2/1         IE - A1 SENDING COMPLETE    Len=0
2005.10.08 11:23:09 L2_FMT BRI 2/1         IE - 04 BEARER CAPABILITY   Len=2
2005.10.08 11:23:09 L2_FMT BRI 2/1              88 Xfer Cap.:UNRESTRICTED DIG.
2005.10.08 11:23:09 L2_FMT BRI 2/1              90 Xfer Rate:64k
2005.10.08 11:23:09 L2_FMT BRI 2/1         IE - 18 CHANNEL ID          Len=1
2005.10.08 11:23:09 L2_FMT BRI 2/1              89 Basic Rate
2005.10.08 11:23:09 L2_FMT BRI 2/1                 Intfc ID:IMPLICIT
2005.10.08 11:23:09 L2_FMT BRI 2/1                 Pref/Excl:EXCLUSIVE
2005.10.08 11:23:09 L2_FMT BRI 2/1                 D-Chan Indicated:NO
2005.10.08 11:23:09 L2_FMT BRI 2/1                 Chan. Sel:B1
2005.10.08 11:23:09 L2_FMT BRI 2/1         IE - 6C CALLING PARTY #     Len=12
2005.10.08 11:23:09 L2_FMT BRI 2/1              21 Numb. Type:NATIONAL
2005.10.08 11:23:09 L2_FMT BRI 2/1                 Numb. Plan:ISDN/Telephony
2005.10.08 11:23:09 L2_FMT BRI 2/1              80 Presentation:ALLOWED
2005.10.08 11:23:09 L2_FMT BRI 2/1                 Ph.# 0009631111
2005.10.08 11:23:09 L2_FMT BRI 2/1         IE - 70 CALLED PARTY #      Len=8
2005.10.08 11:23:09 L2_FMT BRI 2/1              C1 Numb. Type:SUBSCRIBER
2005.10.08 11:23:09 L2_FMT BRI 2/1                 Numb. Plan:ISDN/Telephony
2005.10.08 11:23:09 L2_FMT BRI 2/1                 Ph.# 9633333
2005.10.08 11:23:09 CC_MSG BRI 2/1 CC>>Host: 01 000b SETUP_IND
2005.10.08 11:23:09 CC_IE  BRI 2/1    ie: 00 04 04 80 88 80 90
2005.10.08 11:23:09 CC_IE  BRI 2/1    ie: 00 18 04 80 81 80 81
2005.10.08 11:23:09 CC_IE  BRI 2/1   ie: 00 6C 0E 82 81 80 80 30 30 30 39 36 33 31 31 31 31
2005.10.08 11:23:09 CC_IE  BRI 2/1    ie: 00 70 09 84 81 39 36 33 33 33 33 33
2005.10.08 11:23:09 EP     BRI 2/1 Incoming call :'9633333' from '0009631111'.
2005.10.08 11:23:09 CC_MSG BRI 2/1 Host>>CC: 01 000b CALL_PROCEEDING_REQ
2005.10.08 11:23:09 EP     BRI 2/1 Incoming call to '9633333' accepted
2005.10.08 11:23:09 L2_MSG BRI 2/1 Sent  = FC FF 03 0F 11 25 01 FF
```

Figure 8-26. Viewing ISDN debug Messages

Test Calls

You can also set up a test call to test the ISDN circuit. When you initiate a test call, you connect the two endpoints through an ISDN call without setting up a Data Link Layer connection; test calls only connect at the Physical Layer. When you initiate a test call, the ProCurve Secure Router assigns the BRI interface to ISDN group 0 for the duration of the call.

To set up a test call, enter the following from the BRI interface configuration mode context:

Syntax: test-call [dial <*number*> | answer | hangup]

To enter test call mode, enter:

ProCurve(config- bri 2/1)# test-call answer

This command configures the router to receive test calls.

To dial a test call, enter:

Syntax: test-call dial <*number*>

Replace ***<number>*** with the LDN of the ISDN interface you want to connect to. Enter the LDN without using any special characters. For example, you may enter:

ProCurve(config-bri 2/1)# test-call dial 15555551212

The router will then make a call. Once the test call is connected, the routers will exchange keepalives every 10 seconds.

To disconnect the test call and free the allocated BRI channels, enter:

Syntax: test-call hangup [channels <*channel range*>]

Entering the **hangup** option disconnects the entire ISDN test call. You can also hang up a single B channel by using the **hangup channels** option and specifying on which channel or channels you want to terminate the connection. For example, if you want to hang up both B channels but leave the D channel connected, enter:

ProCurve(config-bri 2/1)# test-call hangup channels 1,2

or

ProCurve(config-bri 2/1)# test-call hangup channels 1-2

To hang up a specific channel, enter the number of the B channel you want to disconnect. For example, if you wanted to hang up channel B2, you would enter:

ProCurve(config-bri 2/1)# test-call hangup channel 2

Test calls allow you to check the physical ISDN connection, end to end, between the calling router and the receiving router.

Line Maintenance

You can also perform some basic maintenance on your ISDN line. Enter:

Syntax: maintenance [restart-d | reset]

Use the **restart-d** option to reset and restart the D channel. This may help in cases where there is a problem in the call process and one of the channels becomes hung.

Use the **reset** option to reset the port hardware. Occasionally the port interface may get into a loop if the disconnect process isn't completed before the connection is lost. To reset all the channels and the port hardware, enter:

```
ProCurve(config-bri 1/1)# maintenance reset
```

Troubleshooting with Loopbacks

A loopback call tests the ability of the router to initiate and terminate an ISDN call, verifying that the ISDN circuit is up and running. To test and diagnose your ISDN lines, you can set loopbacks using the following commands:

Syntax: loopback network [b1 | b2 | both]
Syntax: loopback local [b1 | b2 | all]

Use the **network** option to set a loopback toward the switch. This tests that the line between your router and the switch is operational. Use the **local** option to set a loopback within your local network. This tests whether there is a problem within your LAN that is preventing the connection.

You can specify which B channel you want to test using the **b1**, **b2**, and **both** options. Using the **b1** or **b2** options sets up a loopback call using the channel you specified and the D channel. To test both B channels and the D channel, enter the **all** option.

Troubleshooting PPP for the ISDN Connection

Because PPP is the Data Link Layer for dial-up connections, you may need to troubleshoot the negotiation of a PPP session or PPP authentication (if you have configured authentication for the connections). Table 8-17 lists the **debug** commands you can use to monitor PPP interfaces.

Table 8-17. debug Commands for PPP Interfaces

Command	Explanation
debug ppp verbose	displays detailed information about all PPP frames as they arrive on the PPP interface
debug ppp errors	displays error messages relating to PPP
debug ppp negotiations	displays events relating to link negotiation; shows if link protocols are able to open; reveals when negotiations between two PPP peers fail
debug ppp authentication	displays real-time messages relating to PAP and CHAP
undebug all	turns off debug messages

Quick Start

This section provides the commands you must enter to quickly configure demand routing for:

- an ISDN BRI U module
- an ISDN BRI S/T module

Only a minimal explanation is provided. If you need additional information about any of these options, check "Contents" on page 8-1 to locate the section that contains the explanation you need.

When you configure demand routing, you will need to enter information about your ISDN connection as well as information about the far-end network. You can use Table 8-18 to record this information before you begin to configure demand routing for the ISDN connection.

Table 8-18. Configuration Settings

Setting	Description	Your Setting
interface bri <slot>/<port>	specifies the location of the ISDN module and the port you are configuring	
isdn switch-type [basic-5ess | basic-ni | basic-dms | basic-net3]	specifies the ISDN signaling that the service provider implements on the line	
isdn ldn1 <number> **isdn ldn2 <number>**	specifies the telephone number (or numbers) for ISDN BRI modules	
isdn spid1 <number> <ldn1> **isdn spid2 <number> <ldn2>**	specifies the telephone number and identifiers for each TE on the line; used for ISDN BRI U modules	
connect-sequence <sequence-number> dial-string <string> [<resource-type>] [busyout-threshold <value>]	specifies: • number to call to establish a connection (**dial-string <string>**) • type of connection to establish (**<resource-type>**—ISDN 64 Kbps or ISDN 56 Kbps) • number of times to call the number if a connection cannot be made (**busyout-threshold <value>**)	
ip route <destination A.B.C.D> <subnet mask | /prefix length> <next hop A.B.C.D | forwarding interface ID>	specifies the route to the far-end network	

1. Enter the global configuration mode context:

   ```
   ProCurve> en
   Password:
   ProCurve# configure terminal
   ```

2. Create an access control list (ACL) to define the interesting traffic.
   a. From the global configuration mode context, enter:

      Syntax: ip access-list [standard |extended] <*listname*>

      For example, you might enter:

      ```
      ProCurve(config)# ip access-list extended Call
      ```

   b. From the ACL configuration mode context, configure permit or deny entries. Enter:

      Syntax: [permit | deny] <*protocol*> <*source address*> <*source port*> <*destination address*> <*destination port*> [log | log-input]

      Replace ***<protocol>*** with one of the following:
      – AHP
      – ESP
      – GRE
      – ICMP
      – IP
      – TCP
      – UDP

      To specify the source and destination address, use the following:

      Syntax: [any | host <*A.B.C.D*> | <*A.B.C.D*> <*wildcard bits*>]

      For example, you might want to specify that the interesting traffic is the IP traffic from any source to network 192.168.115.0 /24. You use wildcard bits to specify a range of addresses. Enter:

      ```
      ProCurve(config-ext-nacl)# permit ip any 192.168.115.0 0.0.0.255
      ```

   c. After configuring the entries for the ACL, enter:

      ```
      ProCurve(config-ext-nacl)# exit
      ```

3. Configure the demand interface.
   a. Create the demand interface by entering:

      ```
      ProCurve(config)# interface demand <number>
      ```

      Replace ***<number>*** with a number between 1 and 1024 for this demand interface. Each demand interface must have a unique number.

b. Assign the demand interface an IP address:

Syntax: ip address <*A.B.C.D*> <*subnet mask* | /*prefix length*>

For example, you might enter:

```
ProCurve(config-demand 1)# ip address 10.10.10.1 255.255.255.252
```

or

```
ProCurve(config-demand 1)# ip address 10.1.1.1 /30
```

c. Associate the ACL you created with the demand interface. From the demand interface configuration mode context, enter:

Syntax: match-interesting [list | reverse list] <*listname* > [in | out]

Include the **list** option if you want the ProCurve Secure Router to use standard matching logic for the ACL. Include the **reverse list** option if you want the ProCurve Secure Router to use reverse matching logic when processing the ACL. In this case, the router will try to match the packet's source address with the destination address that is defined in the ACL. The router will then try to match the packet's destination address with the source address that is defined in the ACL.

Replace ***<listname>*** with the ACL that you created to define the interesting traffic. You can specify only extended ACLs.

Including **in** or **out** is optional. By default, the ProCurve Secure Router uses the ACL you specify to check both incoming and outgoing traffic. If you do not specify a direction, outbound traffic is matched to the specified ACL, and inbound traffic is matched to the reverse of the ACL.

For example, if you want to apply the Branch1 ACL to the demand 1 interface, enter:

```
ProCurve(config-demand 1)# match-interesting list Branch1
```

The router will allow both traffic outbound to and inbound from the networks specified in the Branch1 ACL to trigger the dial-up connection.

d. Create a resource pool and associate it with the demand resource. Enter:

```
ProCurve(config-demand 1)# resource pool <poolname>
```

Replace ***<poolname>*** with the name of the resource pool that this demand routing interface will use to originate or answer connections.

e. Configure a connect sequence to specify:

– the telephone number that the demand interface dials to connect to the other remote peer
– the type of dial-up interface used to establish the connection

Enter the following command from the demand interface configuration mode context:

Syntax: connect-sequence <s*equence-number*> dial-string <*string*> [<*resource-type*>] [busyout-threshold <*value*>]

Replace <***sequence-number>*** with a number between 1 and 65535 to identify this set of connection instructions.

Replace ***<string>*** with the telephone number that the demand interface should dial to make the connection.

Replace <***resource-type>*** with one of the options listed in Table 8-19. The option you enter will limit this connection to a particular type of dial-up connection.

Table 8-19. Defining a Resource Type for a Connect Sequence

Option	Description
isdn-64k	Any dial resource can be used, but if ISDN is used, the call must be placed using a 64-Kbps channel.
isdn-56k	Any dial resource can be used, but if ISDN is used, the call must be placed using a 56-Kbps channel.
forced-analog	Only analog resources can be used. (This option is used when you configure demand routing for a backup analog line.)
forced-isdn-64k	Only ISDN resources can be used, and the call must be placed using a 64-Kbps channel.
forced-isdn-56k	Only ISDN resources can be used, and the call must be placed using a 56-Kbps channel.

4. Configure the BRI interface.
   a. To access the BRI interface configuration mode context, enter:

      Syntax: interface bri <*slot*>/<*port*>

      For example, you might enter:

      ProCurve(config)# interface bri 1/1

b. Set the ISDN signaling (switch) type if your service provider is not using the default setting for your ISDN. For the ISDN BRI U module, the default setting is **isdn switch-type basic-5ess**. For the ISDN BRI S/T modules, the default setting is **isdn switch-type basic-net3**. If your service provider is using a different ISDN signaling type, enter:

Syntax: isdn switch-type [basic-5ess | basic-ni | basic-dms | basic-net3]

Table 8-20 lists the command syntax for each signaling type.

Table 8-20. ISDN Signaling Types

Signaling Type	Command Syntax
National ISDN-1	**isdn switch-type basic-ni**
Euro ISDN	**isdn switch-type basic-net3**
Northern Telecom DMS-100	**isdn switch-type basic-dms**
Lucent/ATT 5ESS	**isdn switch-type basic-5ess**

c. Set the LDN. (If your public carrier has assigned you a SPID, skip this step and go to the next step.) Otherwise, enter:

Syntax: isdn ldn1 <*number*>

Replace ***<number>*** with the LDN phone number assigned to the ISDN line you are configuring. For example, you might enter:

```
ProCurve(config-bri 1/1)# isdn ldn1 5555551212
```

d. Set the SPID and LDN. If your public carrier has assigned you a SPID, you should set the SPID and the LDN at the same time. Enter:

Syntax: isdn spid1 <*number*> <*ldn1*>

For example, you might enter:

```
ProCurve(config-bri 1/1)# isdn spid1 12355512120101 5551212
```

e. Activate the interface. Enter:

```
ProCurve(config-bri 1/1)# no shutdown
```

5. Configure an ISDN group.

a. Create an ISDN group by enter the following command from the global configuration mode context:

Syntax: isdn-group <*number*>

Replace ***<number>*** with a number between 1 and 255 to uniquely identify this ISDN group.

b. Assign a BRI interface to the ISDN group. Enter:

Syntax: connect bri <*slot*>/<*port*>

Replace ***<slot>*** and ***<port>*** with the numbers that identify where the BRI interface is installed. You can assign multiple BRI interfaces to the ISDN group. For example, you might enter:

```
ProCurve(config-isdn-group 1)# connect bri 2/1
ProCurve(config-isdn-group 1)# connect bri 2/2
```

c. Assign the ISDN group to a resource pool. From the ISDN group configuration mode context, enter:

Syntax: resource pool-member <*poolname*>

For example, if the resource pool is called Branch, enter:

```
ProCurve(config-isdn-group 1)# resource pool-member Branch
```

Note

The ISDN group can be a member of only one resource pool.

d. To control which calls the BRI interfaces in the ISDN group accept, enter the following command from the ISDN group configuration mode context:

Syntax: incoming-accept-number <*number*>

For example, you might enter:

```
ProCurve(config-isdn-group 1)# incoming-accept-number 5551212
```

You can use the wildcard characters listed in Table 8-9 to specify a range of numbers.

Table 8-21. Wildcard Characters for incoming-accept-number

Wildcard Characters	Explanation
X	Matches any single digit between 0 and 9.
N	Matches any single digit between 2 and 9.
$	Matches any number (multiple numbers).
[ ]	Matches any digit in the list. For example, if you enter [2,4,6] the ProCurve Secure Router matches only 2, 4, and 6. If you enter [4-6,8] the ProCurve Secure Router matches 4, 5, 6, and 8.

6. Create a static route to the far-end network. From the global configuration mode context, enter:

   Syntax: ip route <*destination A.B.C.D*> <*subnet mask* | /*prefix length*> <*next hop A.B.C.D* | *forwarding interface ID*>

   Replace ***<destination A.B.C.D>*** with the IP address for the far-end network. For example, the far-end network might be network 192.168.7.0 /24. Then, either specify the complete subnet mask (such as 255.255.255.0) or enter the prefix length (such as /24). Finally, specify the forwarding interface as demand ***<number>***.

   For example, to configure a route to network 192.168.7.0 /24 through demand interface 1, enter:

   ```
   ProCurve(config)# ip route 192.168.7.0 /24 demand 1
   ```

   For more information about configuring static routes, see "Static Routing" on page 11-9 in *Chapter 11: IP Routing—Configuring Static Routes*.