3

Configuring Backup WAN Connections

Contents

Backing Up Primary WAN Connections

To ensure that users can always exchange data between two offices, you may want to lease a dial-up WAN connection—such as an Integrated Services Digital Network (ISDN) or telephone line—which can be used as a redundant line in case a primary WAN connection fails. Dial-up WAN connections work well as backup connections because you pay only for the time when the connection is in use.

Like other WAN connections, dial-up connections are provided through the public carrier network. In North America, dial-up connections are provided through the public switched telephone network (PSTN). Outside of North America, each country's public telephone and telegraph (PTT) authority provides dial-up connections.

All WAN connections, including dial-up connections, consist of three basic elements:

- the physical transmission media
- electrical signaling specifications for generating, transmitting, and receiving the signals that transmit data through the telephone cables
- Data Link Layer protocols, which provide logical flow control for moving data between the router and the public carrier's central office (CO)

Just as you configure both a Physical Layer and a Data Link Layer for primary WAN connections, you must configure these layers for backup connections. Configuring the Physical and Data Link Layers for backup connections is a slightly different process, however, because you must specify when and how the backup connection is initiated.

Analog Backup Connections

If you want to create a backup connection over the existing telephone cabling, you can use an analog modem, which establishes a dial-up connection to its peer—another analog modem at the remote office. To initiate a physical connection, the analog modem places a telephone call to its peer and then negotiates a logical link with the peer using a Data Link Layer protocol. After the connection is established, the analog modem translates digital data into analog signals. When the two peers are finished exchanging data, the analog modem terminates the connection just as a person would hang up a call.

Analog modems provide comparatively little bandwidth. (The ProCurve Secure Router analog module provides between 300 bps and 33.6 kbps.) When analog modems are incorporated into WAN routers, they are designed only to provide redundancy for other WAN lines, not to furnish a long-term WAN connection.

ISDN-Backup Connections

ISDN is a dial-up WAN connection that supports voice, data, fax, and video services over standard telephone lines. Unlike analog communications, ISDN communications are digital.

Public carriers offer two types of ISDN services:

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

ISDN BRI provides two 64-Kbps bearer (B) channels and one 16 Kbps data (D) channel. The B channels carry data, and the D channel handles the signaling and call control for the ISDN line.

PRI ISDN, on the other hand, provides 23 B channels and 1 D channel in North America and Japan. It provides 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 transmissions to a remote network, or you can use each channel to connect to a different remote office.

Because the ProCurve Secure Router supports BRI ISDN for backup connections, this chapter focuses on BRI ISDN. (The ProCurve Secure Router also supports BRI ISDN for primary WAN connections. For more information, see *Chapter 8: Configuring Demand Routing for Primary ISDN Modules* in the *Basic Management and Configuration Guide*.)

BRI ISDN

BRI ISDN operates over the twisted-pair cabling that is used for ordinary telephones. All of the telecommunications infrastructure that is used to connect your LAN to the CO is collectively called the *local loop*.

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 3-1.) 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.

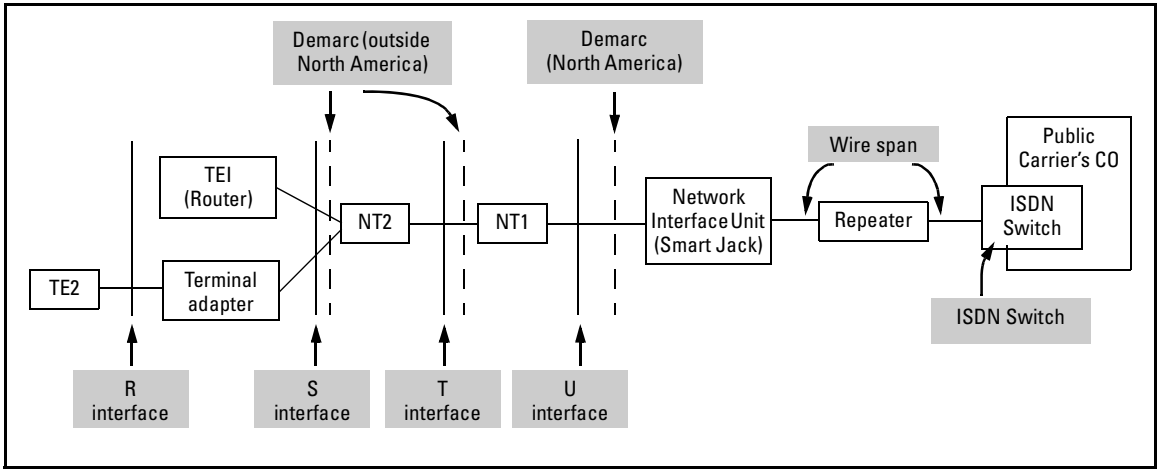

Figure 3-1. ISDN Network

In addition to the demarc, the local loop 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 required only every 5.49 km (18,000 feet). In contrast, T1 encoding requires a repeater approximately every 1.6 km (1 mile or 5,280 feet).

- Wire span—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. Although copper wire has a limited signal-carrying capacity, ISDN is designed to maximize its capability.
- 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.
- NT 2—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.

You do not need to understand all of the equipment used to create the local loop with great technical precision. However, if your ISDN line ever goes down, a basic knowledge and working vocabulary can help you troubleshoot problems with your public carrier.

You should also understand that the demarc defines which equipment your organization is responsible for maintaining. In addition, the demarc determines the type of ISDN backup module you use, as explained in the next section.

ISDN Interfaces. The ISDN standard defines four interfaces, or points, at which equipment can be added to the ISDN network:

- U interface (between the NT1 and the NIU)
- T interface (between the NT2 and the NT1)
- S interface (between the TE1 and the NT2)
- R interface (between the TE2 and the TA)

In Europe, Asia, and all other locations outside of North America, PTTs supply the NT devices. The demarc then falls between the TE (in your case, the router) and the NT1 at the S/T interface. The ProCurve Secure Router provides an ISDN BRI S/T module, which enables a backup interface to connect to either the NT2 or the NT1 provided by your PTT.

In North America, the subscriber must provide the NT devices. The demarc falls between the NT devices and the public carrier's NIU (or smart jack) at the U interface. The ProCurve Secure Router's ISDN BRI U module contains the NT1 and enables a backup interface to function as a U interface.

Electrical Specifications for BRI ISDN

ISDN lines use 2B1Q coding, which uses four signal levels rather than the two of T1- or E1-carrier lines. Each of the four levels, represented by a quaternary, corresponds to a combination of two bits. For example, the signal level for 1 followed by 1 is different for that of 1 followed by 0. This coding scheme allows BRI ISDN lines to compress data. Also, 2B1Q operates at a lower frequency range than T1/E1 encoding and sustains fewer losses with fewer repeaters.

Backup Modules for the ProCurve Secure Router

All narrow Data Link modules on the ProCurve Secure Router provide an extra port for a backup interface. To activate the backup interface, you must purchase and install one of the following backup modules:

- analog
- ISDN BRI U
- ISDN BRI S/T

The ProCurve Secure Router supports BRI ISDN, which provides a transmission rate of 64 Kbps or 128 Kbps. The analog module on the ProCurve Secure Router supports between 300 bps and 33.6 Kbps.

As Figure 3-2 shows, the backup module is installed over the data link module.

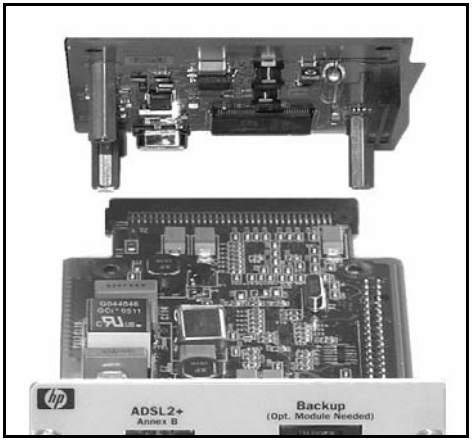

Figure 3-2. Installing a Backup Module

After the backup module is installed, it can back up any interface on the router, not only those interfaces installed in the same slot. You can back up:

- Point-to-Point Protocol (PPP) connections
- High-level Data Link Control (HDLC) connections
- Frame Relay connections
- ISDN primary connections
- Asymmetric Digital Subscriber Line (ADSL) connections
- Internet connections (using any Data Link Layer protocol)

Standards

On the ProCurve Secure Router, both ISDN backup 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 specifies 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 to these three options, the ISDN BRI S/T backup 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.

You must configure your router's BRI interface for the type of signaling your service provider implements. Because switches can implement various types of signaling depending on their software, the signaling type will not always be that of the CO switch's manufacturer.

Data Link Layer Protocols

On the ProCurve Secure Router, backup ISDN connections always use PPP as the Data Link Layer protocol, no matter what Data Link Layer protocol is used for the primary connection. For example, if the ISDN line is used to back up a Frame Relay connection between two offices, the ISDN uses PPP.

Determining a Backup Method

The ProCurve Secure Router initiates a backup connection in response to a backup condition. Backup conditions include Layer 1, or Physical Layer, failures such as:

- T1 and E1 alarms
- ADSL failure due to low signal-to noise ratio (SNR)
- other line failures and WAN alarms

Backup conditions also include Layer 2, or Data Link Layer, failures such as:

- signaling failure
- loss of permanent virtual circuit (PVC)

You have two choices for configuring how the ProCurve Secure Router responds to a backup condition:

- You can configure demand routing, which is activated only if *both* of the following conditions are met:
  - A backup condition occurs, bringing the primary interface down.
  - The router receives traffic that must be transmitted to the far-end network.

- You can configure a persistent backup connection, which is initiated immediately if a backup condition occurs on the primary connection and stays up until the primary connection is available again.

Before you configure a backup connection, you should evaluate your network environment and then determine which option best meets your company's particular needs.

Using Demand Routing for Backup Connections

Demand routing allows you to capitalize on the main advantage of a dial-up connection: it establishes the dial-up connection when it is needed and terminates the connection when it is no longer necessary. For example, you may lease an ISDN line to serve as the backup WAN connection between the main office and a branch office. If the primary interface goes down and no one is transmitting traffic, you may not want the backup WAN connection to become active. This type of usage would substantially increase your company's telephone costs. Instead, you may want to establish the ISDN connection only when two conditions are met:

- the primary interface goes down
- traffic must be transmitted between the two offices

Demand routing only establishes the backup connection when traffic is sent from the main office to the branch office and the primary interface is unavailable. (See Figure 3-3.)

In addition to establishing the connection only when it is needed for data transmission, demand routing ensures that when the dial-up connection is idle for certain amount of time, the ProCurve Secure Router terminates the call. You can configure the idle timer to match the rates you are charged for the ISDN line. For example, if your service provider charges your company for every two minutes that the ISDN line is established, you can set the idle timer to 110 seconds. The ProCurve Secure Router will then disconnect the ISDN line when it has been idle for 110 seconds, and your company will not be charged for an additional two minutes.

With demand routing, you can also be very selective in the type of traffic that causes the router to initiate the ISDN connection. For example, you can limit this "interesting" traffic to packets sent from one subnet to another subnet. You can also exclude routing updates (if you are using a routing protocol) and other traffic that you do not think is essential. Carefully selecting the type of traffic that triggers an ISDN connection limits the amount of time that your company uses its ISDN connection, thereby decreasing costs.

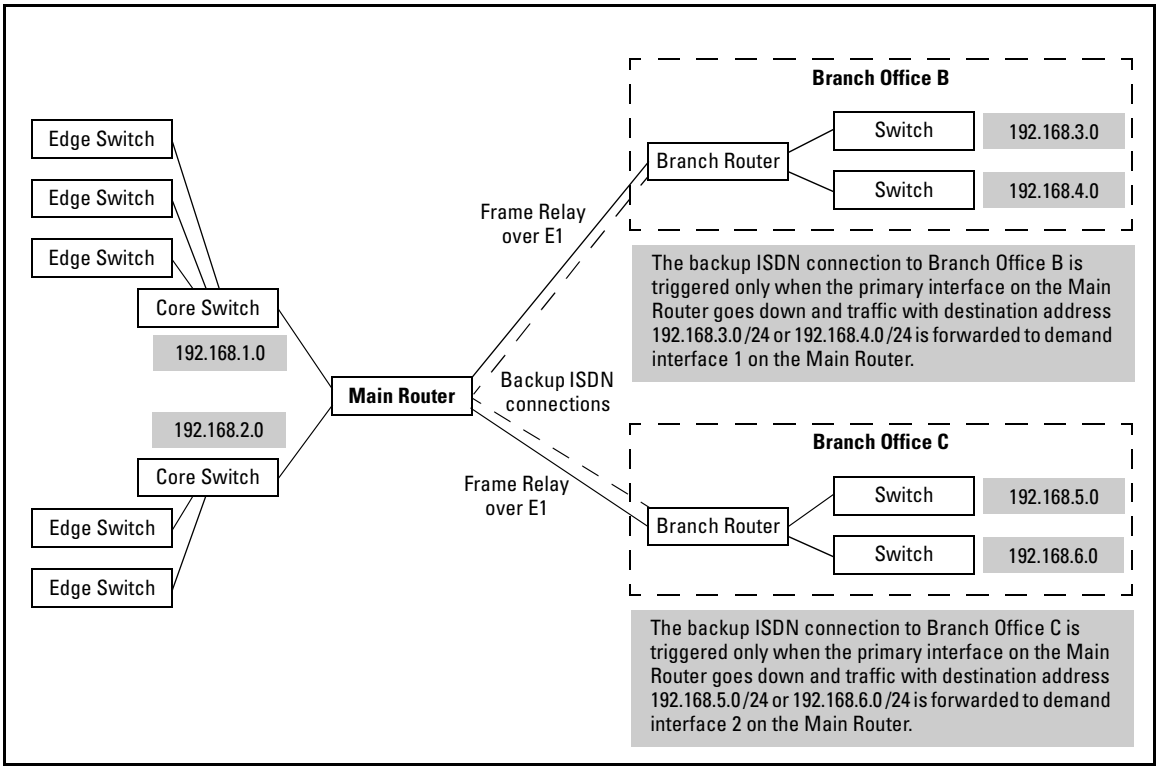

Figure 3-3. Using Demand Routing for Backup Connections

Demand routing has another advantage: it supports two-port ISDN modules. If you are not using all of the narrow slots in your ProCurve Secure Router, you can purchase a two-port ISDN module and use it as a primary WAN connection or as a backup to other primary WAN connections. To use the two-port module for backup connections, you follow the instructions outlined in *Chapter 8: Configuring Demand Routing for Primary ISDN Modules* in the *Basic Management and Configuration Guide*, with one exception. Rather than creating a static route to the far-end network, you create a floating static route, ensuring that the administrative distance for this floating static route is higher than the administrative distance for the route through the primary interface. For more information about static routes, see "Configuring a Floating Static Route for a Persistent Backup Connection" on page 3-69.

If you purchase this two-port ISDN module, you can use Multilink PPP (MLPPP) to aggregate channels across ISDN lines, increasing bandwidth for the dial-up connection.

If you use the backup ISDN modules, you cannot use MLPPP to aggregate channels. The ISDN backup modules support bonding, rather than channel aggregation. You can bond channels on an ISDN backup module only if:

- you configure a persistent backup connection
- the router connects to another ProCurve Secure Router

If both of these conditions are met, you can use bonding to increase bandwidth.

Note

If you use demand routing with a backup ISDN module, you can neither bond nor multilink channels.

Using Persistent Backup Connections

You can also configure the backup module so that it immediately establishes a dial-up connection when the primary interface fails. This connection stays up until the primary interface is available again. You may want to configure this type of backup connection between offices that require a constant connection.

The ProCurve Secure Router provides some settings to control when a persistent backup connection is established. For example, you can prevent the connection from becoming active on weekends or evenings.

As mentioned earlier, when you configure a persistent backup connection, you can bond two B channels for a total of 128 Kbps. The only limitation is that the router must connect to another ProCurve Secure Router. If you want to use MLPPP to aggregate channels, you must purchase and use a two-port ISDN module, as described in *Chapter 8: Configuring Demand Routing for Primary ISDN Modules* in the *Basic Management and Configuration Guide*.

Comparing Demand Routing and Persistent Backup Connections

Table 3-1 lists the main differences between demand routing and persistent backup connections.

Table 3-1. Differences Between Demand Routing and Persistent Backup Connections

Option	Demand Routing	Persistent Backup Connection
supported hardware	• analog and BRI backup modules, which can be installed on top of any narrow module • two-port ISDN modules, which are installed in a narrow slot on the ProCurve Secure Router	analog and backup modules, which can be installed on top of any narrow module
applications	• backup modules—backup WAN connection for two offices that require high availability but need to limit usage and costs • two-port ISDN modules—WAN connection between two offices that exchange data periodically and need a low-cost WAN solution	backup for two locations that must maintain a constant WAN connection
Data Link Layer protocol	PPP, which is configured through the demand interface	PPP, which is configured through a PPP interface
initiation of dial-up connection	• backup connection—established when two conditions are met: – primary connection is unavailable – "interesting" traffic needs to be transmitted • primary ISDN connection—established when "interesting" traffic must be transmitted	backup connection established immediately when the primary connection fails and maintained until the primary connection is re-established
termination of dial-up connection	• backup connection—terminated when primary connection is re-established or when no interesting traffic is received before the idle timer expires • primary connection—terminated when no interesting traffic is received for the time specified in the idle timer	terminated when primary connection is re-established
methods to limit usage of dial-up connections	• configure the access control list (ACL) to limit "interesting" traffic, which triggers the ISDN connection • adjust idle timers to match the time intervals for which your company is charged for its dial-up connection	specify times, such as weekends and evenings, when the dial-up connection should not be established (even if the primary connection goes down)
increasing bandwidth	• no bonding or MLPPP support for ISDN backup modules • MLPPP support for two-port ISDN modules	channel bonding with another ProCurve Secure Router

Figure 3-4 shows how a backup connection is established if demand routing is configured. Figure 3-5 shows how a persistent backup connection is established.

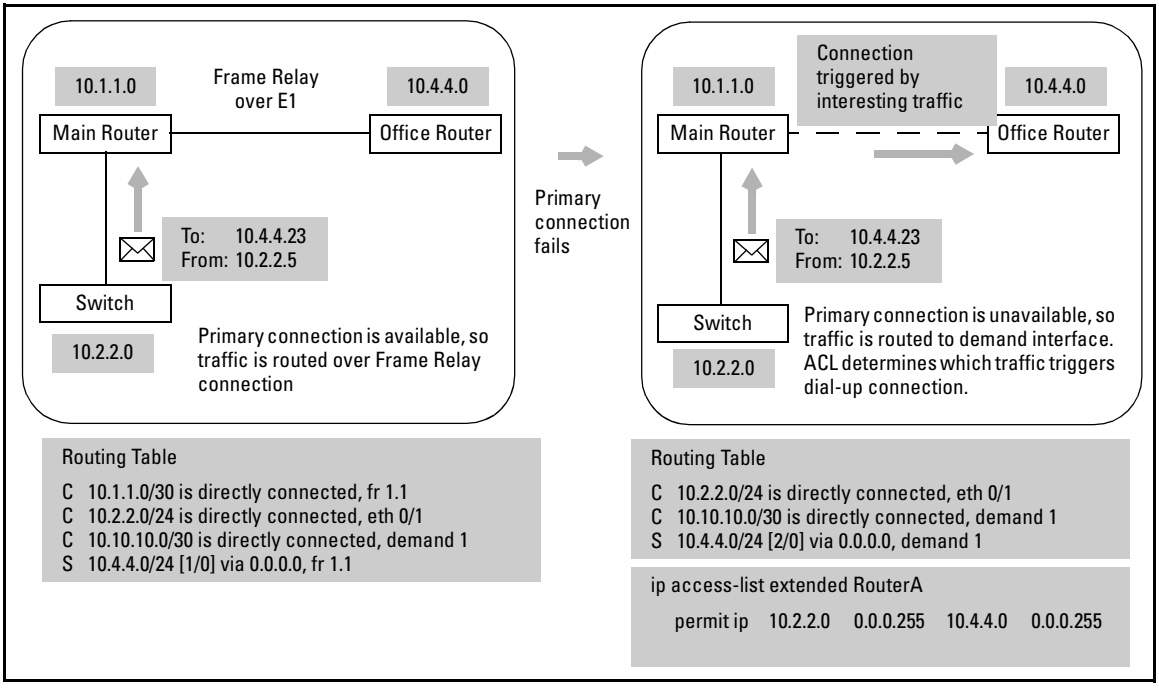

Figure 3-4. Demand Routing for a Backup Connection

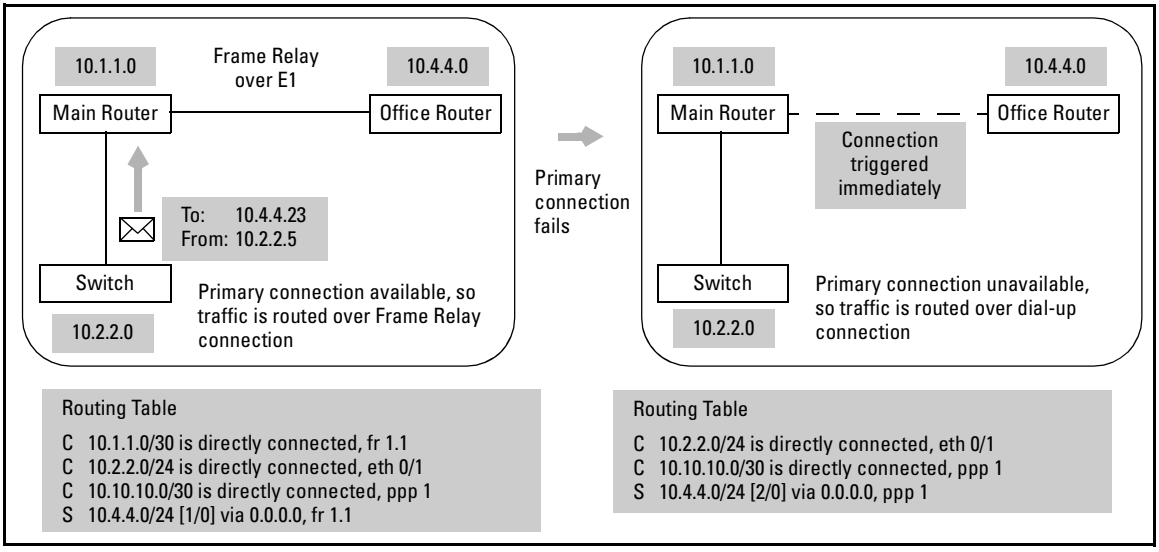

Figure 3-5. Persistent Backup Connection

If you want to use demand routing for your backup connections, continue with the next section. If you want a persistent backup connection, continue with "Configuring a Persistent Backup Connection" on page 3-49.

Configuring Demand Routing for Backup Connections

To configure demand routing for backup connections, 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 when the primary interface is unavailable.
2. Configure a demand interface.
3. Configure the BRI interface.
4. Create a floating static route to the far-end network.

Define the Traffic That Triggers the Connection

You must first define the interesting traffic—the traffic that triggers, or activates, the WAN connection. For example, if you are configuring demand routing for a backup connection between the main office and a branch office, the interesting traffic would be the packets destined for the branch office. The ProCurve Secure Router will route these packets to the demand interface only if the primary interface is down and the floating static route that you configure for the traffic is activated in the routing table. (Floating static routes are explained in more depth later in this chapter.)

To define the interesting traffic, you create an extended ACL. The ProCurve Secure Router will use this ACL to identify and select interesting traffic.

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 and can enter permit and deny 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*> [<*packet bits*>] [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 a number between 0 and 255 for the protocol.

For demand routing, you may want to create an ACL that selects all 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 first the source address and then the destination address, using the following syntax for each address:

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

Table 3-2 lists the options you have for specifying a source or destination address.

Table 3-2. Options for Specifying Source and Destination Addresses

Option	Meaning
any	match all hosts
host <A.B.C.D>	specify a single IP address or a single host
hostname <hostname>	specify a single host, using a hostname rather than an IP address
<A.B.C.D> <wildcard bits>	specify a range of IP addresses

Using Wildcard Bits. You use wildcard bits to permit or deny a range of IP addresses. Wildcard bits define which address bits the Secure Router OS should match and which address bits it should ignore.

When you enter wildcard bits, you use a zero to indicate that the Secure Router OS should match the corresponding bit in the IP address. You use a one to indicate that the Secure Router OS can 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
```

If you enter **192.115.1.0** 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 with the address 192.115.1.0 /24. (For more information about configuring ACLs, see *Chapter 5: Applying Access Control to Router Interfaces*.)

Examples. For example, if you want any traffic to the far-end network 192.168.115.0 /24 to trigger the dial-up connection, you would 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, use wildcard bits to specify that network as the source. For example, enter:

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

Implicit "Deny Any" for ACL. 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.

After you have finished creating the ACL, enter **exit** to return to the global configuration mode context.

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.

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.

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 the pool of dial-up interfaces used for backup.

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 also create routes to any of the networks connected through a dial-up interface. When the ProCurve Secure Router detects traffic that must be routed through a demand interface, it processes the extended ACL that has been applied to it to select interesting traffic. If the traffic matches that ACL, the router attempts to establish the dial-up connection.

After the physical connection is established, the ProCurve Secure Router uses PPP as the Data Link Layer for the dial-up connection. To ensure that backup connections are only established with authorized routers, 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 the 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 **connect-sequence** settings.
7. Configure timers, caller, and hold queue settings (optional).
8. Configure caller settings (optional).

You must complete steps 1-6. Steps 7-8 are optional.

Creating the Demand Interface

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

Syntax: interface demand <*number*>

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

After you create the demand interface, its status automatically changes to administratively up. You do not need to activate the interface by entering **no shutdown**. The demand interface will begin spoofing an up status after you configure an IP address for it.

Configuring an IP Address

You have several options for setting up an IP address on the demand interface: 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. The demand interface will then 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 take its address include:

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

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, enter:

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

To view the routing table, enter:

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

Figure 3-6 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 3-6. A 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. This option eliminates the need to create another ACL for return traffic. 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.

Outbound interesting traffic triggers the demand interface to initiate the dial-up link. Outbound interesting traffic also resets the idle timer on an active link. (The idle timer determines how long the ISDN connection can remain up if no traffic is transmitted over it.) Inbound interesting traffic only resets the idle timer.

If you include the **in** option when you enter the **match-interesting** command, the ProCurve Secure Router will use the specified list to select inbound interesting traffic. If you include the **out** option, the router will determine whether the traffic outbound through the interface is interesting.

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

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

When you view the demand interface in the running-config, you will see two commands, even though you entered only one. (See Figure 3-7.)

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

Figure 3-7. The match-interesting Command as Displayed in the Running-Config

Entering the following two commands would accomplish the same thing as entering **match-interesting list Backup**:

```
ProCurve(config-demand 1)# match-interesting list Backup out
ProCurve(config-demand 1)# match-interesting reverse list Backup 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 dial-up 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 3-36 and "Configuring the fast-idle Option" on page 3-36.)

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 3-3 shows each option and when you would use it. The default setting is **either**.

Table 3-3. 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 you want the demand interface to originate a call when it receives interesting traffic, you must set the **connect-mode** to **originate** or **either**.

If you want the demand interface to answer backup calls from a remote peer, you must set the **connect-mode** to **answer** or **either**.

You could also configure the demand interface so that the **match-interesting** command selects outbound traffic and the **connect-mode** command is set to **answer**. In this mode, the router will not use demand routing to initiate a backup connection. However, interesting outbound traffic will keep a 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. The **match-interesting** command controls both the traffic that triggers a connection and the traffic that will reset the idle timer.

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 dial-up interfaces. The **resource pool** command creates a resource pool and associates it with the demand interface. Each demand interface can be associated with only one resource pool.

To 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 calls.

This resource pool is empty until you assign backup interfaces to it.

Defining a 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 one dial-up line that you are using for backup. 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 3-4. The option you enter will limit this connection to a particular type of dial-up connection.

Table 3-4. Defining a Resource Type for Connection Instructions

Option	Description
isdn-64k	Any dial resource can be used, but if ISDN is used, the call must be placed using 64 KB.
isdn-56k	Any dial resource can be used, but if ISDN is used, the call must be placed using 56 KB.
forced-analog	Only analog resources can be used.
forced-isdn-64k	Only ISDN resources can be used, and the call must be placed using 64 KB.
forced-isdn-56k	Only ISDN resources can be used, and the call must be placed using 5 6 KB.

For example, if you are using ISDN backup, 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 between 1 and 65535 to specify the maximum number of times the ProCurve Secure Router will try this connect sequence. 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 3-30.)

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

Deleting a Connect Sequence. To delete a connect sequence entry**,** enter:

ProCurve(config-demand 1)# no connect-sequence <*sequence-number*>

Specify the Order in Which Connect Sequences Are Used

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

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

Table 3-5 lists each option with a brief description.

Table 3-5. 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 no connection has been made, process the first connect sequence.)

The default setting is **sequential**. To return the **connect-order** to the default setting, 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 that are configured for a demand resource 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 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 the connect-sequence interface-recovery Option

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

A Dial-Up 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 Dial-Up Interfaces Are Available. Backup interfaces on the ProCurve Secure Router are not directly bound to a specific primary connection. You could use a dial-up interface to provide backup for multiple connections. If no dial-up interface in the associated resource pool is available for use when the demand interface determines that it must initiate a backup connection, the ProCurve Secure Router places all interfaces in the resource pool in fast-idle mode. This mode decreases the amount of time an interface can remain idle before the router disconnects the ISDN connection. The router then monitors the dial-up interfaces until one becomes available. When an 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 3-36.)

A Dial-Up Interface Is Available, But the Call Fails. If a dial-up 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

Because you can configure a number of settings for connect sequences, it is important to understand how these settings interrelate. For example, consider the configuration shown in Figure 3-8.

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

Figure 3-8. Connection Instructions for a Demand Interface

The resource pool for this configuration contains two members: a BRI interface and a modem interface. If the primary interface for a connection goes down and interesting traffic is forwarded to this demand interface, the ProCurve Secure Router will first process connect sequence 10, which requires an ISDN connection. If the BRI interface is available, Figure 3-8 shows that the ProCurve Secure Router will try to call 5551212.

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

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 3-8, the ProCurve Secure Router will make three activation attempts—that is, it will process all connect sequence 10 up to nine times and connect sequence 20 up to three times.

If all three attempts are unsuccessful, the ProCurve Secure Router will change the status of the demand interface to “down (recovery active).” It will then remove the IP address and any routes referencing the interface, allowing any routes with higher metrics to take their place.

In 60 seconds, the ProCurve Secure Router will try to process the **c**onnect sequences again (although the demand interface will remain down in recovery active mode). If that attempt is unsuccessful, the ProCurve Secure Router will try again in 60 seconds. Based on the configuration in Figure 3-8, 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 intervene by shutting down the demand interface or clearing the connection. If the demand interface succeeds in establishing the backup connection, 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 that use the interface.

Figure 3-9 summaries this process.

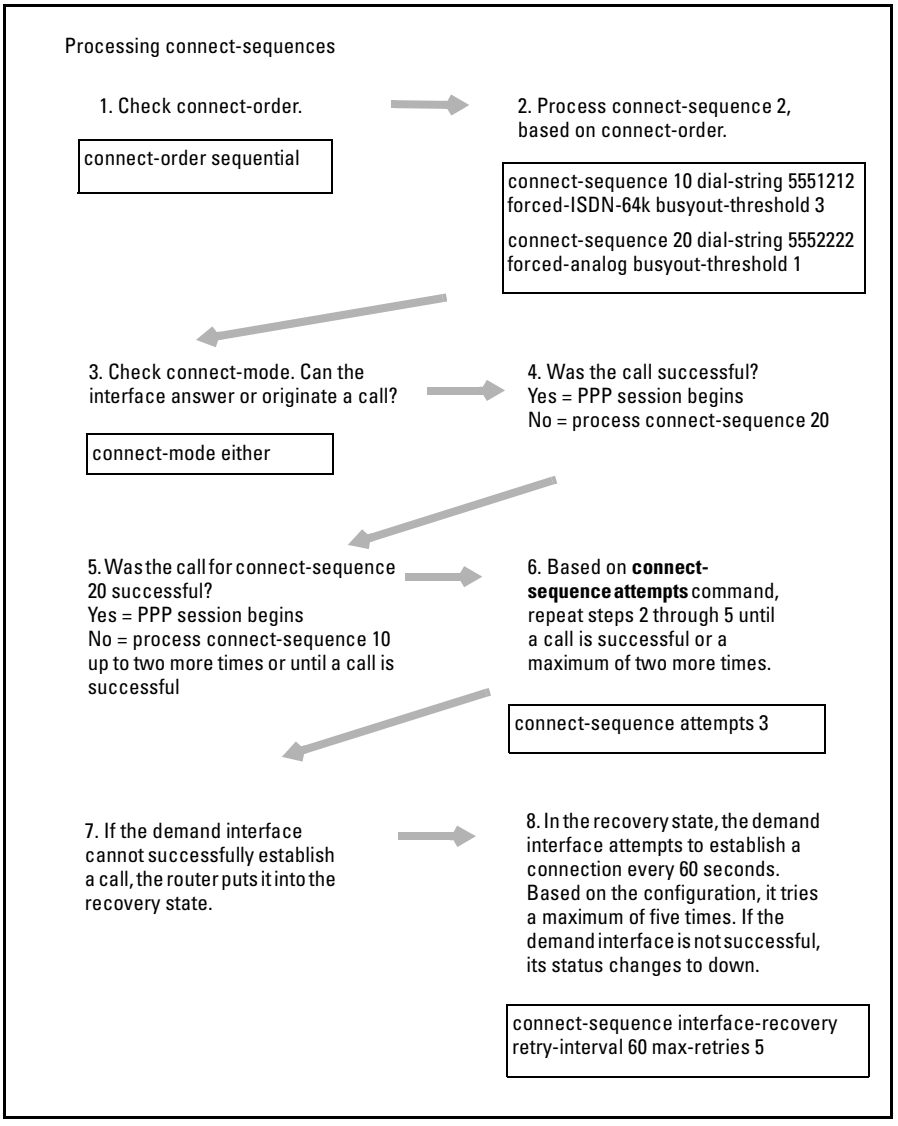

Figure 3-9. Understanding the connect Commands for Demand Routing

Configuring the idle-timeout Option

You can configure the amount of time that the demand interface remains up in the absence of interesting traffic. The idle timer helps to keep the backup connection cost-effective: backup is only active when it is truly necessary. To decrease your company's costs, you should configure the **idle-timeout** setting to match the rates your public carrier charges for the ISDN (or analog) line. For example, if your public carrier charges you for every two minutes of usage, you should set the **idle-timeout** setting to be 120 seconds or just slightly less than 120 seconds. That way, the backup connection will be terminated before your company is charged for another two-minute time interval.

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. 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 a backup interface is in use and is needed to establish another connection, the **fast-idle** option determines the number of seconds that the connection will remain up in the absence of interesting traffic. Because the interface is 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

When an ISDN or analog call is established, the calling party supplies a Calling Line ID (CLID). If you configure a **caller-number**, the backup interface will check the CLID when it receives calls. If the CLID matches the **caller-number** you specified, the interface will answer the call. If the two numbers do not match, the interface will not answer the call.

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

From the demand interface configuration mode context, enter:

Syntax: caller-number <*CLID*>

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

By default, no **caller-number** is specified.

Defining the called-number

You can also configure the Dialed Number Identification Service (DNIS) that the ISDN or analog 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 or modem interface to provide when answering or making a call.

Again, you can enter multiple **called-number** commands.

By default, no **called-number** is specified.

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 or Modem 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 interface an LDN if you are using a BRI S/T interface, or assign the BRI interface a SPID and LDN if you are using a BRI U interface module.
4. Assign the BRI interface to the resource pool you created for the demand interface.
5. Activate the BRI interface.

If you are configuring a modem interface, you:

1. Access the modem interface configuration mode context.
2. Specify the country code.
3. Assign the interface to the resource pool you created for the demand interface.
4. Activate the modem interface.

Accessing the BRI or Modem Interface

To access the configuration mode context for the BRI or modem interface, enter:

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

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

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

The port number you enter depends on the location of the module you are configuring. For modules that have only one WAN port, the backup port is port 2. For modules that have two WAN ports, the backup port is port 3.

For example, if the module is located in slot 1 and you are configuring the ISDN backup interface in port 3, enter.

```
ProCurve(config)# interface bri 1/3
```

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 switches. Rather than simply configuring the BRI interface for a particular ISDN switch, you actually 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 3-6 lists the command syntax for each signaling type.

Table 3-6. 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 an LDN for ISDN BRI S/T Modules

The LDN is the PTT or PSTN number that the router calls to reach the public carrier and establish the WAN link. When the router receives a WAN connection call through the public carrier, it identifies the far-end caller using the LDN. Unless you set an LDN, the interface cannot answer calls. It can, however, still place calls if the service provider supports connections without an LDN. However, the peer might not answer the calls if it has been configured to require a caller ID.

Note

As of release J.04.01, the ProCurve Secure Routers can use the **isdn ldn1** command to set the LDN for ISDN BRI S/T modules. It is no longer necessary to use the **isdn spid1** command (and enter 0000 for the SPID) to set the LDN for these modules.

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 in North America, you may also need to define a SPID. As described in the next section, you can set the SPID at the same time that you set the LDN.

Configuring a SPID and LDN for ISDN BRI U Modules

Some North American telcos, principally those that use the ISDN switches DMS-100 and National ISDN-1, issue a SPID, which is typically a 14-digit number that includes the interface's 10-digit telephone or directory number 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
```

Note

In North America, 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 these commands.

Setting the Country for the Modem Interface

Depending on what country your router is in, your modem may need to use different signals to connect to the public carrier network. You must identify the country for the analog module from the global configuration mode context:

Syntax: modem countrycode <*country*>

For example, you might enter:

```
ProCurve(config)# modem countrycode Germany
```

Enter **modem countrycode ?** for a complete list of keywords for countries. The default setting is USA and Canada.

Assigning BRI or Modem Interface to the Resource Pool

To assign backup interfaces to the resource pool, enter the following command from the BRI or modem interface configuration mode context:

Syntax: resource pool-member <*pool name*> [<*cost*>]

Replace ***<pool name>*** with the name of the resource pool that this interface will join.

Replace ***<cost>*** with a number between 1 and 255 to assign a priority to the resource pool. The default setting is **1**.

An interface can be a member of more than one resource pool. If an interface belongs to two resource pools and is requested simultaneously by both, the ProCurve Secure Router will use the **cost** option to determine which resource pool can use the interface. If both resource pools are assigned the same **cost**, the ProCurve Secure Router will use alphabetical order to determine which resource pool can use the interface. That is, if the name of one resource pool is Branch and the name of the other resource pool is Main, the router will assign the interface to the Branch resource pool.

For example, to assign the BRI 1/3 interface to the resource pool named "backup," enter:

```
ProCurve(config)# interface bri 1/3
ProCurve(config-bri 1/3)# resource pool-member backup
```

To remove an interface from a resource pool, enter the following command from the interface configuration mode context:

Syntax: no resource pool-member <*poolname*>

Activating the Interface

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

Syntax: no shutdown

Caller ID Options for ISDN BRI Backup Modules (Optional)

The ProCurve Secure Router accepts ISDN calls based on whether the incoming call's caller id matches a list of acceptable caller ids. You can override an incoming call's caller id using the **caller-id override** option. Enter:

Syntax: caller-id override [always | 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 all incoming caller ids 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 a Floating 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. For backup connections, you create a floating static route, which is activated only when the primary route is not available.

To configure a floating static route to the far-end network, you must enter the following information:

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

To configure an IP 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*> [<*administrative distance*>]

For example, to configure a route to network 192.168.7.0 /24 through demand interface 1 and assign this route an administrative distance of 2, enter:

```
ProCurve(config)# ip route 192.168.7.0 /24 demand 1 2
```

This route appears in the routing table only if another route with a lower administrative distance is not available. For example, Figure 3-10 shows the routing table for a network if the primary WAN connection to network 192.168.7.0 /24 is available. Figure 3-11 shows the routing table for the same network if the primary interface to 192.168.7.0 /24 is not available.

```
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    10.10.10.0/30 is directly connected, ppp 2
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    192.168.7.0/0 [1/0] via 0.0.0.0, ppp 2
```

IP route through primary interface

Figure 3-10. Routing Table if the Primary Interface Is Available

```
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    192.168.7.0/0 [2/0] via 0.0.0.0, demand 1
```

IP route through backup interface

Figure 3-11. Routing Table if the Primary Interface Is Unavailable

Note

The ProCurve Secure Router supports network monitoring, which can provide a mechanism for detecting failed static routes (the primary route). With the network monitoring feature, you can create a track to monitor the primary route using network monitor probes. If the route should fail, network monitoring removes it, and the floating static route is added to the routing table. For more information about network monitoring, see the *Advanced Management and Configuration Guide*, *Chapter 9: Network Monitoring*.

Configuring PPP Authentication for an ISDN Connection

If you want to ensure that only authorized PPP peers can establish a 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.

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, you must configure the username and password that the ProCurve Secure Router sends when the far-end router requests authentication information for a dial-up 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 for a dial-up 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.

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.

Example of Demand Routing with PAP Authentication for a Backup Connection

Figure 3-12 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-username** command configures the username and password that the ProCurve Secure Router will send its peer.

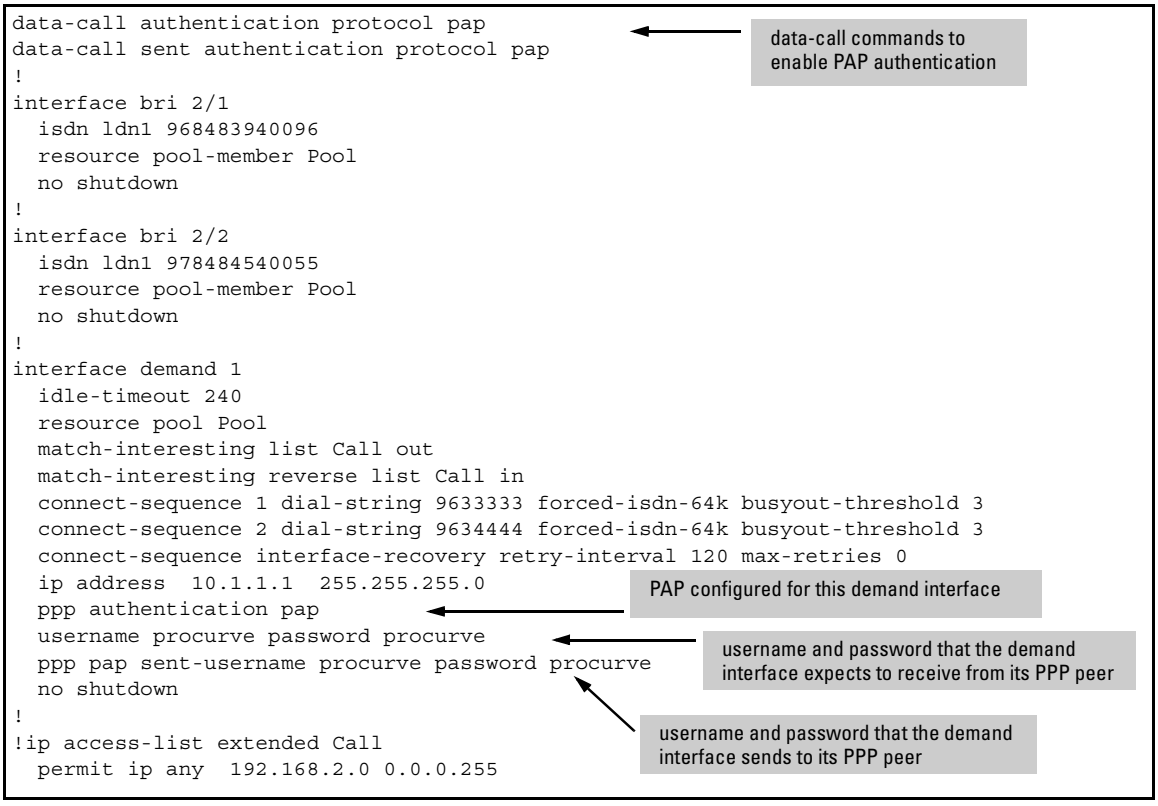

Figure 3-12. Using PAP Authentication with Demand Routing

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.

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 a Persistent Backup Connection

If your company needs a constant WAN connection between two offices, you should configure a persistent backup connection. Then, if the primary connection fails, the persistent backup connection will be established immediately, and it will remain up until the primary WAN connection is available again.

To set up a persistent backup connection, you configure:

- a physical interface (the BRI or modem interface)
- a logical interface (which is a PPP interface) for the backup connection
- backup settings on the logical interface for the primary WAN connection

Configuring the Physical Interface for a Persistent Backup Connection

For persistent backup connections, you can configure a BRI interface for ISDN lines or a modem interface for an analog connection over a regular telephone line.

Configuring a BRI Interface (ISDN Only)

For a BRI interface, you must configure:

- ISDN signaling type
- local directory number (LDN)
- service profile ID (SPID) for North America only

You must also activate the interface.

Accessing the Configuration Mode Context. To begin configuring the BRI interface, move to the BRI interface configuration mode context:

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

For example, you might enter:

```
ProCurve(config)# interface bri 1/3
```

Setting the ISDN Signaling (Switch) Type. The BRI interface must implement the same type of ISDN signaling that your public carrier uses. (See "Electrical Specifications for BRI ISDN" on page 3-9 to learn more about the standards supported by the ProCurve Secure Router.) The signaling type does not necessarily have to be that of the CO switch's manufacturer. For example, a Lucent switch can implement National ISDN-1 signaling. Your telco should inform you which signaling method it uses.

Consult Table 3-7 for the command syntax that implements each signaling type.

Table 3-7. 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**

For example, to set the signaling type to National ISDN-1, enter:

```
ProCurve(config-bri 1/3)# isdn switch-type basic-ni
```

The default settings are:

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

Setting the LDN (Outside North America). The LDN is the local number that remote routers call to reach the local router through the ISDN connection. The peer at the other end of the connection includes this number in its backup dial list. Unless you set an LDN, the interface cannot answer calls. It can, however, still place calls if the public carrier supports connections without an LDN. However, the peer might not answer the calls, depending on the its Caller ID settings.

To set the LDN, enter:

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 in North America, you may also need to define a SPID. As described in the next section, you can set the SPID at the same time that you set the LDN.

Setting the SPID and LDN (North America). Some North American telcos, principally those that use the DMS-100 and National ISDN-1 switches, issue SPIDs. A SPID is typically a 14-digit number that includes the BRI interface's 10-digit phone number and several identifiers. These identifiers specify the type of service on the line, indicating that the interface accepts data rather than voice.

Even though the SPID typically includes the LDN, you must specify the LDN separately after the SPID if you want the interface to answer calls. Enter the following command:

Syntax: isdn spid1 <*SPID*> <*LDN*>

Enter the LDN that your public carrier provides. For example:

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

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

Syntax: isdn spid2 <*SPID2*> <*LDN2*>

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

Syntax: no shutdown

You can check the status of the interface by entering:

Syntax: do show int bri <*slot*>/<*port*>

The status should be "ready." The report will also show you the settings you have entered for signaling, SPID, and LDN. (See Figure 3-13.)

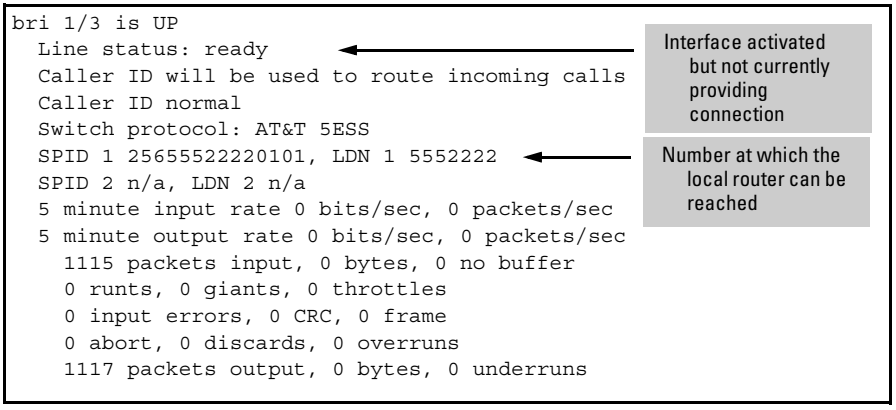

Figure 3-13. Viewing the Status of an BRI Interface

Configuring Timers for Bonded ISDN Calls. If you bond two channels to increase bandwidth for a backup ISDN connection, you can configure a number of timers for the bonded connection. You configure these timers from the BRI interface configuration mode context, although you enter the command to enable channel bonding when you configure a backup call list. See "Adding a Number to a Backup Dial List" on page 3-65.

Note

The two-port ISDN modules support MLPPP for channel aggregation. The backup ISDN modules support channel bonding if you configure a persistent backup connection to another ProCurve Secure Router.

You can configure the bonding timers listed in Table 3-8.

Table 3-8. BONDing Commands

Command Syntax	Function	Default Value in Seconds
bonding txadd-timer	aggregate call timeout	50
bonding txcid-timer	B channel negotiation timeout	5
bonding txdeq-timer	network delay equalization timeout	50
bonding txfa-timer	frame pattern detection timeout	10
bonding txinit-timer	origination endpoint negotiation timeout	10
bonding txnull-timer	answering endpoint negotiation timeout	10

The **txadd-timer** command specifies the length of time the router will wait for additional calls to be connected before deciding that the bonding call has failed. When dialing overseas, you should enter a value above 60 seconds to allow for slower call routing.

Syntax: bonding txadd-timer <*seconds*>

The **txcid-timer** command sets the maximum amount of time the router will take to negotiate data rates and channel capacities for the bearer channels.

Syntax: bonding txcid-timer <*seconds*>

When multiple calls are being aggregated, the calls may be routed through different devices within the public carrier's infrastructure. This can create a delay between the two calls.

The **txdeq-timer** command sets a maximum amount of time for the router to take when equalizing the delay between the two calls that are being bonded.

Syntax: bonding txdeq-timer <*seconds*>

The **txfa-timer** command specifies the length of time the originating and answering routers spend attempting to detect the bonding frame pattern when a call is connected.

Syntax: bonding txfa-timer <*seconds*>

The **txinit-timer** option sets the time the *originating* router waits to detect the bonding negotiation frame pattern when a call is connected.

Syntax: bonding txinit-timer <*seconds*>

The **txnull-timer** command specifies the time the *answering* router takes attempting to detect the bonding negotiation pattern from the originating router. It may be necessary to shorten this timer if the DTE equipment using the bonding module also has timer constraints for negotiating a non-bonding parameter.

Syntax: bonding txnull-timer <*seconds*>

Configuring a Modem Interface (Analog Only)

To configure a modem interface, you must:

- identify your country
- activate the interface

Optionally, you can:

- replace incoming caller ID with a set number
- use the modem for console dial-in

Setting the Country. Depending on where the router is located, the analog backup module may need to use different signals to connect to the PSTN or PTT. You must identify the country for the analog module from the global configuration mode context:

Syntax: modem countrycode <*country*>

For example, if the router is in Munich, Germany, enter:

```
ProCurve(config)# modem countrycode Germany
```

Enter **modem countrycode ?** for a complete list of keywords for countries. The default setting is USA and Canada.

For the rest of the configuration commands, you must access the modem configuration mode context.

Activating the Interface. The modem interface must be manually activated. First, access the modem interface:

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

For example, you might enter:

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

The slot refers to the slot number for the module on top of which you installed the backup module. The port is the port number for the backup interface on this dl module.

Activate the interface by entering:

Syntax: no shutdown

You can check the status of the interface by entering:

```
ProCurve(config-modem 1/2)# do show int mod 1/2
```

The status should be "UP" and "on-hook." Activating the backup interface does *not* activate the actual backup connection; it only enables backup support.

Using the Modem for Console Dial-In

You can connect to the analog module on the ProCurve Secure Router and initiate a console session with it.

Caution

If you enable dial-in console sessions, you cannot use the module for backup.

To use the modem for dial-in console sessions, enter:

```
ProCurve(config-modem 1/2)# dialin
```

Replacing Incoming Caller ID for BRI and Modem Interfaces

You can replace the incoming caller's ID with a number of your choosing. You can do so for all calls or only for calls that do not have a caller ID. If you replace the caller ID with the number configured in a backup dial list, the analog module will answer all calls.

This command allows the router to answer calls from a peer that has no caller ID.

Note

Use care when overriding caller IDs, particularly when the primary interface's call mode allows the router to always answer backup calls. If you override the caller ID security check, the router may establish a connection with an unauthorized peer. To prevent this, you can also configure PPP authentication.

To override the caller ID, enter this command from the interface configuration mode context:

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

The **if-no-CID** option assigns the number only to peers with no caller ID. The **always** option assigns the number to all peers.

For example, if you want the router to assign peers with no caller ID the number 5551112, enter:

```
ProCurve(config-modem 1/2)# caller-id override if-no-CID 5551112
```

Configuring a Logical Interface for a Persistent Backup Connection

Although a backup connection provides redundancy for a primary WAN connection such as a Frame Relay connection or an ISP connection, it does *not* duplicate the primary WAN connection. The backup connection is ultimately to the same peer, but it is established through a different path in the PSTN or PTT infrastructure. For example, Frame Relay running over an E1- or T1-carrier line establishes a fixed path through the PSTN or PTT infrastructure. If that connection is lost, the backup connection must be established using a different path through the PSTN or PTT infrastructure. (See Figure 3-14.)

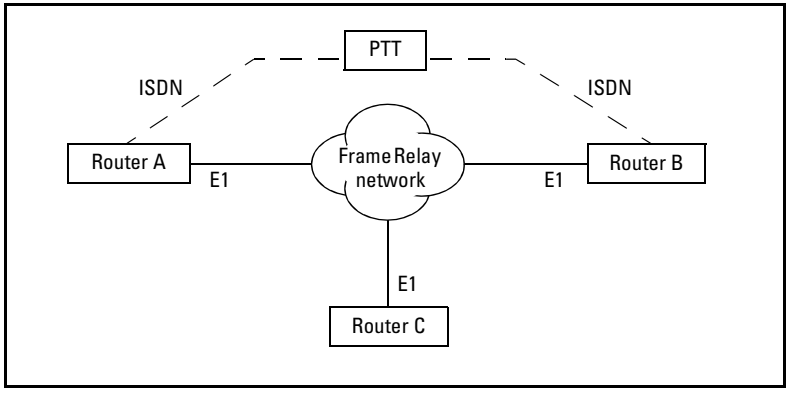

Figure 3-14. Backing Up a Frame Relay Connection

The dial-up connection through the physical PSTN or PTT network needs a Data Link Layer protocol to establish the new link and regulate the flow of data. Just as for any other WAN connection on the ProCurve Secure Router, you configure the Data Link Layer protocols in a logical interface. However, unlike for ADSL, T1, and E1 connections, you do not explicitly bind the backup line to a logical interface. Instead, you configure a backup logical interface, which you then map to the logical interface for the primary connection. When the primary interface goes down, the backup interface establishes a connection using whatever backup line is available.

On the ProCurve Secure Router, PPP provides the Data Link Layer for persistent backup connections. You configure a backup PPP interface no matter what type of Data Link Layer protocol, including Frame Relay or Asynchronous Transfer Mode (ATM) (which is used for ADSL connections), is used for the primary connection.

A backup interface is simply a supplemental PPP interface that you create and configure as you would any PPP interface. You must configure an IP address for the backup PPP interface. For best security practices, ProCurve Networking also recommends that you configure PPP authentication.

You do *not* configure the number that the backup interface will call, nor whether the interface will answer or place backup calls (or both), from the backup interface configuration mode context. You enter these configurations for each primary connection from its logical interface configuration mode context. For example, if the primary connection is Frame Relay running over a T1-carrier line, you would enter these configurations from the Frame Relay subinterface configuration mode context.

Creating a Backup PPP Interface

To create the backup interface, enter the following command from the global configuration mode context:

Syntax: interface ppp <*interface number*>

For example, to create PPP 2, enter:

```
ProCurve(config)# int ppp 2
```

The backup PPP interface only provides backup; you cannot use it for a primary WAN connection. The backup PPP interface, like the backup line, can provide redundancy for more than one WAN connection.

You can also configure a separate PPP interface for each primary WAN connection—for example, when your peers have different authentication settings. If the router contains more than one than backup module, you should configure a separate backup PPP interface for each module. Both backup modules can then be active at the same time.

Activating the Interface

The PPP interface cannot make or receive backup calls unless it has been manually activated. Enter:

```
ProCurve(config-ppp 2)# no shutdown
```

Setting an IP Address

The backup interface's IP address must be on a different network than that of the primary connection. (The router does not allow more than one interface to be on the same network.) To configure the IP address, enter this command from the backup PPP interface configuration mode context:

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

For example, if the primary connection were on network 10.1.1.0 /30, you could assign the following address to the backup interface:

```
ProCurve(config-ppp 2)# ip address 10.10.10.1 /30
```

The peer's backup IP address will also be on a different network than the primary connection. If you are using static routing, you must configure a floating static route to the remote network through the backup interface. See "Configuring a Floating Static Route for a Persistent Backup Connection" on page 3-69.

Enabling PPP Authentication

The ProCurve Secure Router that answers a backup call uses caller ID to ensure that it only connects calls from authorized peers. This prevents the router from making an expensive backup connection with a random caller. In addition, you should consider having the router that originates the backup call require PPP authentication. Authentication ensures that the backup number called still belongs to an authorized peer. (You can also configure the answering router to request authentication.)

The ProCurve Secure Router supports PAP or CHAP authentication for the backup connection.

Requiring Authentication From the Peer. To require PAP authentication from the peer:

1. Move to the configuration mode for the backup PPP interface.
2. Enable PAP authentication:

   ```
   ProCurve(config-ppp 2)# ppp authentication pap
   ```

3. Add the peer's username and password to the PPP database:

   Syntax: username <*peer's username*> password <*peer's password*>

   For example, you could enter:

   ```
   ProCurve(config-ppp 2)# username london password procurve
   ```

To require CHAP authentication from the peer:

1. Move to the configuration mode for the backup PPP interface.
2. Enable CHAP authentication:

   ProCurve(config-ppp 2)# ppp authentication chap

3. Add the peer router's hostname and password to the PPP database:

   ProCurve(config-ppp 2)# username LondonRouter password procurve

Providing Authentication to the Peer. If the remote router's backup interface requires authentication, you must configure the backup interface with the correct authentication information.

To configure a PAP username and password:

1. Move to the configuration mode for the backup PPP interface.
2. Enter the username and password you have received from your peer:

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

   If you are backing up a connection to an ISP, the username and password will probably be the same as those you received for the primary connection. For example, enter:

   ProCurve(config-ppp 2)# ppp pap sent-username NewYork password procurve

To configure a CHAP username and password:

1. Move to the configuration mode for the backup PPP interface.
2. Enter the password you have received from your peer:

   Syntax: ppp chap password <*password*>

   If you are backing up a connection to an ISP, this will probably be the same password that you received for the primary connection. For example, enter:

   ProCurve(config-ppp 2)# ppp chap password procurve

3. The router automatically sends its hostname. If your peer has assigned you a different username than your hostname, enter:

   Syntax: ppp chap hostname <*username*>

Configuring Persistent Backup Settings for a Primary Connection

Even though you install a backup module in a specific module slot, the corresponding backup line can provide redundancy for any of the WAN connections on the router. You enable backup for a connection by configuring a backup dial list on the primary connection's logical interface.

For the primary logical interface, you must configure:

- backup call mode
- a backup dial list:
  - peer's number
  - the type of backup connection
  - backup interface

You can also configure:

- times at which backup support is enabled
- backup intervals and timers

Accessing the Primary Connection's Logical Interface

Move to the logical interface associated with the primary connection to access the **backup** commands.

Syntax: interface <*interface ID*>

You can configure backup for these interfaces:

- PPP interfaces
- Frame Relay subinterfaces
- ATM subinterfaces
- HDLC interfaces
- tunnel interfaces

For example, if the logical interface for the primary connection is Frame Relay 1.101, enter:

```
ProCurve(config)# int fr 1.101
```

Note

You configure separate backup connections for every PVC in a Frame Relay network or ATM connection. Therefore, you enter the **backup** commands from the Frame Relay or ATM *subinterface*. The analog or ISDN line can only provide active backup for one PVC at a time. Analog and ISDN lines establish a point-to-point connection to another router.

Setting the Backup Call Mode

The role a router takes in the backup call process depends on the backup call mode you assign to the primary connection's logical interface. If you allow the connection to originate calls, the router will, by default, initiate the dial-out process 10 seconds after the connection fails. (You can change this default waiting interval. See "Setting Backup Timers" on page 3-68.) It will then begin the dial-out process described below.

If you allow the router to only answer calls, it will wait to receive a call to back up the connection. The router will then begin the dial-in process described in "Dialing In" on page 3-63.

Dialing Out. When the Secure Router OS places a backup call, it follows these steps (see Figure 3-15):

1. The Secure Router OS places an outbound call, dialing the number stored in the backup dial list. This list is configured individually in the logical interface for each primary connection. The name and number of the backup PPP interface (the logical interface that maintains the backup connection) are also stored in the backup dial list. For example, if the backup PPP interface is PPP 2, PPP 2 is stored in the primary interface's backup dial list with the number the PPP 2 interface should call for backup. This number is that of the analog or BRI module on the router on the other side of the connection. (See Figure 3-16.)

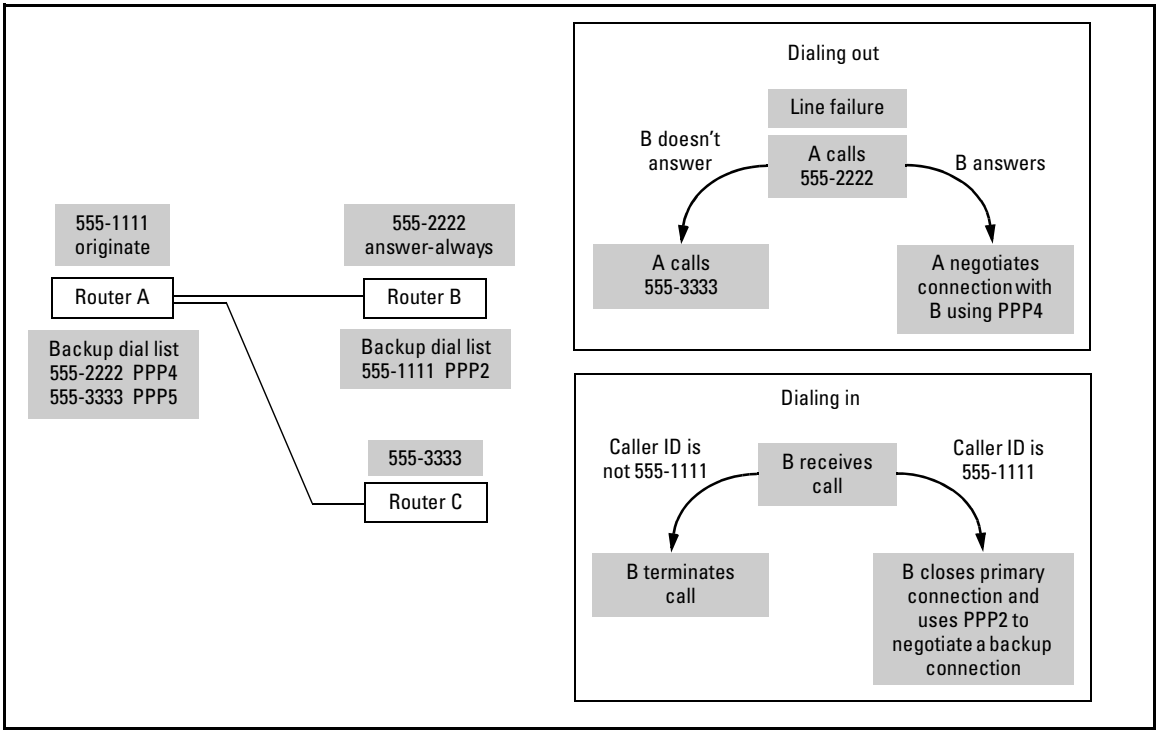

Figure 3-15. Backup Call Process

2. If the peer answers the call, the Secure Router OS sends the authentication and negotiation protocols that have been configured for the backup PPP interface. If the authentication and negotiation are successful, the backup connection is established.

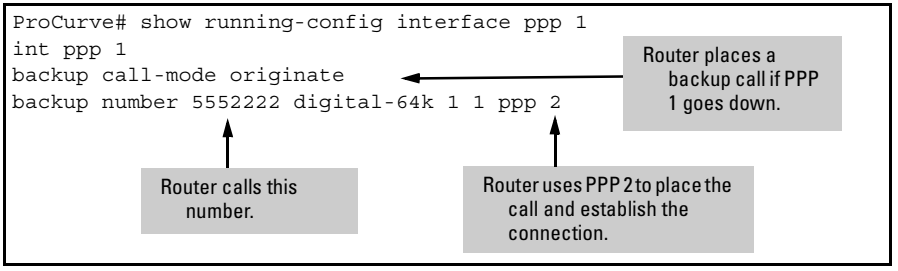

Figure 3-16. Backup Settings for Dialing Out

3. If the call fails to connect, the Secure Router OS checks the backup dial list in the primary interface for a second number, which references a different backup PPP interface. If there is a second number, the Secure Router OS attempts to connect to it.

Dialing In. When the Secure Router OS receives an inbound call, it follows these steps (see Figure 3-15):

1. It uses caller ID to compare the call's number with the backup dial list number configured for the PPP interface. (See Figure 3-17.)
2. If the numbers match, the Secure Router OS connects the call. The primary link may already be down. However, you can also configure an interface to answer backup calls even when its own primary connection is up. In this case, the Secure Router OS closes the primary connection and connects the backup call.
3. If the inbound call does not match a number in the backup dial list number, the Secure Router OS terminates the call.

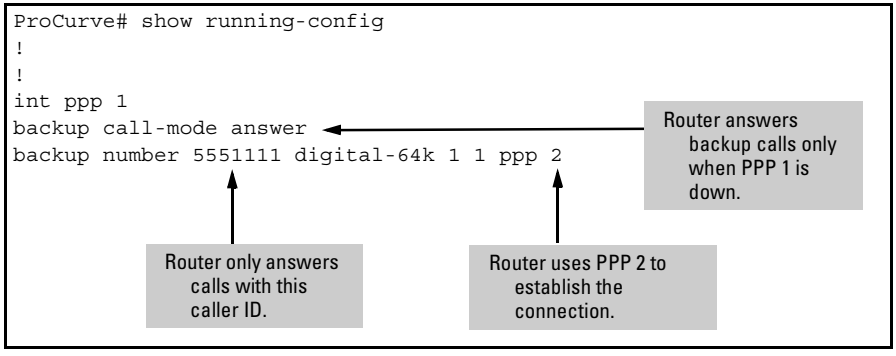

Figure 3-17. Backup Settings for Dialing In

The primary connection's logical interface can allow its backup interface to originate calls, answer them, or both. At least one side of the connection must be able to originate calls, and at least one side must be able to answer them.

Refer to Table 3-9 for all available backup call modes and the commands to configure them.

Table 3-9. Backup Call Modes

Command Syntax	Description
backup call-mode answer	If the primary connection fails, the backup interface will answer backup calls but not place them.
backup call-mode answer-always	The backup interface will always answer backup calls, even when the primary connection is up.
backup call-mode originate	If the primary connection fails, the backup interface will place a backup call; it will not answer a call.
backup call-mode originate-answer	If the primary connection fails, the backup interface will place *or* answer a call. It refuses calls when the primary connection is up.
backup call-mode originate-answer-always	If the primary connection fails, the backup interface will place *or* answer a call. It will also answer backup calls when the primary connection is still up.

Note

When a connection's backup call mode is set to either **answer-always** or **originate-answer-always**, the ProCurve Secure Router will force a functional primary connection down in favor of the backup connection. You should use this option for sites that are not directly connected.

For example, in Figure 3-18 Router A acts as a hub in a Frame Relay network. Router B's T1 connection fails, and it places a call to Router A. Router A's T1 lines are still good, and its PVC to the Frame Relay provider may still be up. If the subinterface is only set to **answer**, the router will not answer the call, and the connection to Router B will be lost. However, if the Frame Relay 1.102 subinterface is set to back up call mode **answer-always**, the backup interface will force PVC 1.102 down and bring up the backup connection.

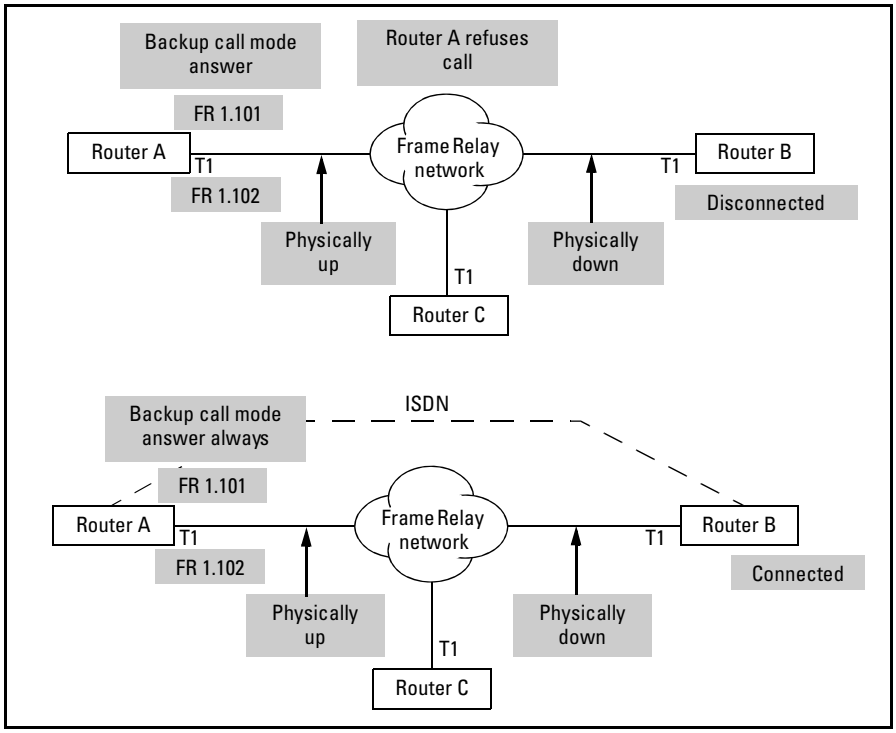

Figure 3-18. Backup Call Mode on a Frame Relay Network

Adding a Number to a Backup Dial List

Each logical interface stores its own backup dial list, which enables backup for the connection. You can store more than one number in the backup dial list. For each number, the list stores the following:

- Number—If the backup call mode includes **originate**, the backup interface calls this number when the primary connection fails. If the call mode includes **answer**, the number also acts as caller ID. Any inbound call must match this number in order for the Secure Router OS to connect the call.
- Backup type—Depending on the backup module you have installed, you can select:
  - analog
  - digital (ISDN) 56 K
  - digital (ISDN) 64 K

For digital modules, you *must* also specify whether the ISDN line will use a single channel (56 or 64 Kbps) or a bonded channel (112 or 128 Kbps). You do so by entering the minimum and maximum DS0 or E0 channels.

Note

Bonding calls is a proprietary feature. You can only establish bonded calls between two ProCurve Secure Routers.

- Backup interface—The backup interface is the PPP interface that actually originates and/or answers the backup call and maintains the backup connection. The backup dial list is where you map a primary interface to its backup interface.

To configure the backup dial list, enter the following command from the primary connection's logical interface:

Syntax: backup number <*peer's LDN*> [analog | digital-56k | digital-64k] [1 1 | 1 2] ppp <*backup interface number*>

For example, if the remote site's number is 555-2222 and the routers use an ISDN backup module, enter:

```
ProCurve(config-ppp 1)# backup number 5552222 digital-64k 1 2 ppp 2
```

You use the **1 1** option for an ISDN line that uses a single channel. The **1 2** option is for a bonded call.

You can add more than one number to the list. If the peer with the first number does not answer within the connect timeout interval (see Table 3-10 on page 3-69), the router calls the second number. The router tries numbers in the order that you enter them.

Note

By default, the router retries the first backup number an unlimited number of times even if you have configured a second number. If you want the router to try the second number, set a number of times for the router to try the first. (See "Setting Backup Timers" on page 3-68.)

Controlling When a Backup Connection Can Be Established

Because backup connections are dial up, you pay for them only when they are active. You should specify the times that backup support is enabled so that a connection does not become active when it is not needed. For example, your organization may be closed over the weekend. If a WAN connection fails on Friday night and a backup connection is allowed to come up, your company will be charged for two days of a connection that no one was using.

You do not actually *activate* the backup connection by specifying times when a backup connection can be established. Rather, you enable the router to establish a backup connection *if* the primary connection fails during those times.

Day. Use the **backup schedule day** command to set the days when backup is enabled. From the primary connection's logical interface, enter:

Syntax: [no] backup schedule day [sunday | monday | tuesday | wednesday | thursday | friday | saturday]

By default, backup is enabled at all times for any connection with at least one number in its backup dial list. You should use the **no** option to disable backup for a connection on certain days. For example, to turn off backup on the weekends, enter:

```
ProCurve(config-ppp 1)# no backup schedule day saturday
ProCurve(config-ppp 1)# no backup schedule day sunday
```

Enter the command *without* the **no** option to re-enable backup on that day.

Time. You can also specify the times of day when a connection is backed up. For example, you may want to turn backup off at night. Enter the time when backup support should be turned off:

Syntax: backup schedule disable-time <*hh:mm:ss*>

Enter the hours in 24 hour format. For example, you might enter:

```
ProCurve(config-ppp 1)# backup schedule disable-time 18:00:00
```

Next, enter the time when backup support should be turned back on.

Syntax: backup schedule enable-time <*hh:mm:ss*>

For example, you might enter:

```
ProCurve(config-ppp 1)# backup schedule enable-time 7:00
```

Caution

Make sure that your router is set with the correct time and date. From the enable mode context, enter:

```
ProCurve# show clock
```

If you need to configure the router to receive time from an SNTP server, enter the following command from the global configuration mode context:

Syntax: sntp server [<*hostname*>|<*A.B.C.D*>] [version <*1-3*>]

If you want to manually set the clock, enter the following command from the enable mode context:

Syntax: clock set <*hh:mm:ss*> <*day*> <*month*> <*year*>

Setting Backup Timers

You can alter the timers that control settings such as the delay between line failure and backup initialization, between redial attempts, and before primary line reestablishment.

The default settings are adequate for most applications. However, if both sides of the connection are allowed to originate calls, you should randomize timers. When the connection fails, both peers will try to call each other at the same time, causing a *call collision* or *contention*. (This is the "busy" signal.) Randomizing the timers minimizes the risk of routers calling each other at the same time and receiving a busy signal. Enter:

```
ProCurve(config-ppp 1)# backup randomize-timers
```

You can view a complete list of **backup** commands by entering **backup ?** from the logical interface configuration mode context. Refer to Table 3-10 for a list of default backup settings and timers and the commands to alter them.

Table 3-10. Backup Timers

Command Syntax	Function	Default	Range
backup auto-backup | no backup auto-backup	automatic backup initiation after a connections fails	on	—
backup backup-delay <seconds>	time between line failure and placing a backup call	10 seconds	10-86,400 seconds (1 day)
backup connect-timeout <seconds>	time the router waits for a call to connect	60 seconds	10-300 seconds *recommended over 60
backup redial-delay <seconds>	time between redial attempts (either to the same or a new number)	10 seconds	10-600 seconds (1 hour)
backup maximum-retry <attempts>	number of times the router will attempt a call	unlimited	0-15 *0 means unlimited
backup auto-restore | no backup auto-restore	automatic restoration of a primary connection after it comes back up	on	—
backup restore-delay <seconds>	time before restoring a primary connection after it comes back up	10 seconds	10-86,400 seconds (1 day)

Configuring a Floating Static Route for a Persistent Backup Connection

A backup interface must be on a different subnet than its primary interface. This means that traffic will need to follow a different route to reach the same destination. If you use a dynamic routing protocol, the router can learn this route on its own. You must remember to activate the routing protocol on the backup network.

However, if you use only static routing, you must enter a backup route to the remote network through the backup interface.

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*> [<*administrative distance*>]

For example, you might enter:

ProCurve(config)# ip route 192.168.64.0 /18 ppp 2 2

You can specify the local backup interface as the forwarding interface to ensure that the route will be accurate even if the peer changes its backup IP address. If you do enter a next hop address, remember that this address should be that of the peer's backup interface, which like the local backup interface, is on a different network from the primary connection. (See Figure 3-19.)

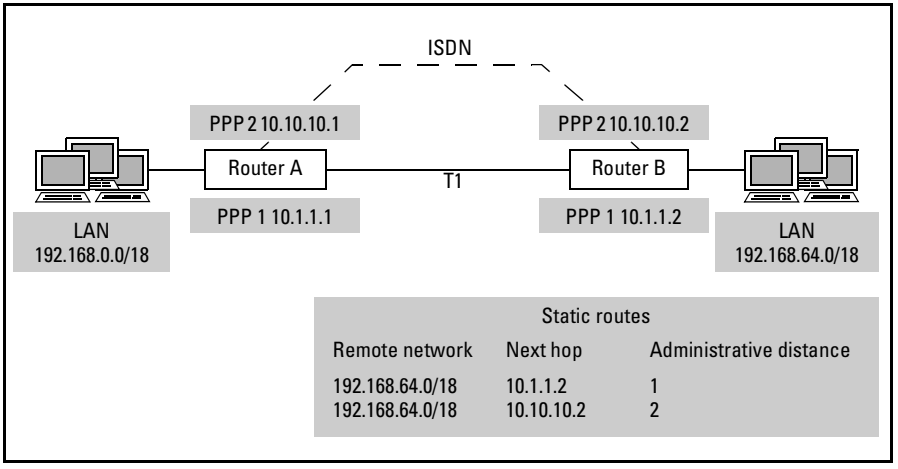

Figure 3-19. Floating Static Route

The floating static route is a different path to a destination for which you have already entered a static route. You should configure the administrative distance to **2** (as opposed to the default **1** for static routes). The route will then not be added to the route table unless the primary route becomes invalid (the primary connection fails).

Figure 3-20.

Note

The ProCurve Secure Router supports network monitoring, which can provide a mechanism for detecting failed static routes (the primary route). With the network monitoring feature, you can create a track to monitor the primary route using network monitor probes. If the route should fail, network monitoring removes it, and the floating static route is added to the routing table. For more information about network monitoring, see the *Advanced Management and Configuration Guide*, *Chapter 9: Network Monitoring*.

You may have configured a default route to your ISP through a forwarding interface. If you are backing up your Internet connection, remember to add a floating default route through the backup interface.

Note

If your router uses routing protocols to learn routes to the remote destination, you must enter an administrative distance for the floating static route that is higher than the administrative distance for the routing protocol. For example, the administrative distance for OSPF routes is 110, so you could enter this command:

```
ProCurve(config)# ip route 192.168.64.0 /18 ppp 2 120
```

Configuring Persistent Backup for Multiple Connections

A single analog or ISDN module can back up any number of connections, although, of course, it can only *actively* back up one failed connection at a time. To enable backup on multiple connections simply configure a backup dial list for each connection.

Special considerations for backing up multiple connections include:

- setting a connection's priority
- configuring multiple backup interfaces

Priority. A connection's relative priority determines which connection a backup module serves when more than one connection goes down at a time. By default, every connection for which backup has been configured has a priority of 50. The router will back up the connection with the higher priority value.

In a Frame Relay network, a backup line can only provide a connection for one PVC at a time. If your router has a Frame Relay WAN connection with multiple PVCs, you should set the highest priority for the most mission critical PVC.

To set the priority for a connection, move to the logical interface configuration mode context for that connection. Enter this command:

Syntax: backup priority <*priority*>

A connection's priority can be between 0 and 100, with 100 the highest priority.

Multiple Backup Interfaces. You can use the same backup interface for more than one connection, but you should configure a separate backup interface for each connection when using authentication. A PPP interface can only store one username and password in its database. If the peers for the different connections have different usernames, you need to create and configure a separate backup PPP interface for each. Map the backup interface to the primary interface in the primary interface's backup dial list.

Viewing Backup Configurations and Troubleshooting Backup Connections

The steps you take to view and troubleshoot backup connections vary, depending on whether you are using demand routing or persistent backup connections. Because both configurations rely on the same backup modules, however, there is one common area: the BRI or modem interface.

This section first describes how to view information about BRI and modem interfaces and how troubleshoot any problems at the Physical Layer. This section is then divided into two subsections:

- "Viewing Information about Demand Routing and Troubleshooting Problems" on page 3-77
- "Viewing Information about Persistent Backup Connections and Troubleshooting Problems" on page 3-86

Viewing Information about BRI and Modem Interfaces and Troubleshooting Problems

Whether you are using demand routing or a persistent backup connection, you can use the bank of LEDs on the front panel of the ProCurve Secure Router to quickly determine the status of a backup module. Depending on the model of your router, the bank will include 8 or 11 LEDs. The backup LEDs, which are in the second row, display information about the backup modules. The LED in the first column reports on the module installed in the first module slot, and the LED in the second column reports on the module installed in the second module slot.

Table 3-11 explains how to interpret the LEDs' signals.

Table 3-11. Backup LEDs

Color	Meaning
off	The backup interface has not been activated.
red	The backup interface is down.
solid green	The backup interface is up and ready to provide a connection.
flashing green	The backup interface is active and providing the current connection.

Viewing the Status and Configuration of Backup Interfaces

After you configure backup support, you should verify that the BRI or modem interface is ready to provide the backup connection, and you should double-check the configuration. For BRI interfaces, you should ensure that the BRI interface has been configured with the correct settings for the ISDN switch (signaling) type, LDN, and SPID (if one is required). If you are using demand routing, you should also ensure that the BRI or modem interface has been assigned to a resource pool.

View the Status of the BRI Interface. To check the configuration and the status of the BRI interface, enter the following command from the enable mode context:

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

You can also add **do** to access the commands from any mode context. For example, you can view the status of a BRI interface while configuring that interface by entering:

```
ProCurve(config-bri 1/2)# do show interface bri 1/2
```

The first line of the display reports the status of the interface and of the ISDN line. (See Figure 3-21.)

```
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 3-21. Viewing the Status of a BRI Interface That Is in Use

For example, it might report: "bri 1/2 is UP." The line status should be "ready." See Table 3-12 to learn what different BRI line statuses mean.

Table 3-12. BRI Interface Line Status

Line Status	Meaning
ready	The interface is up and ready to provide backup.
connected	The interface is active and providing the current connection.
disconnected	The interface is up, but has disconnected from the peer. The backup settings for the primary interface or settings in the demand interface may prevent the call from connecting.
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.

If the interface is down, you must bring it up before the module will be ready to back up connections.

The status report also includes:

- switch protocol (ISDN signaling type)
- SPIDs and LDNs
- packet statistics and errors

Verify that the SPID(s) and/or LDN(s) are correct. If you are located in North America, double-check whether your public carrier has assigned you one or two SPIDs. When you use both B channels, public carriers that use National ISDN and Northern Telecom DMS-100 sometimes require you to configure a SPID for each channel.

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

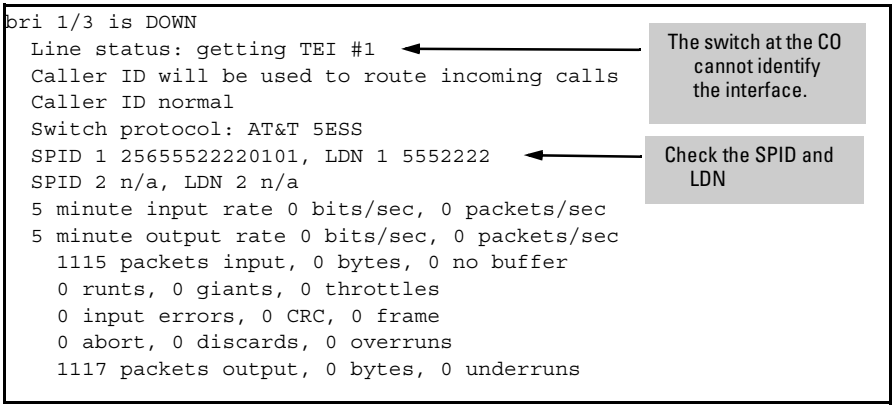

Figure 3-22. Troubleshooting a BRI Interface

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

The line status indicates the point at which this process derails. For example, in Figure 3-22, the line status indicates that the CO switch is attempting to get the BRI interface's SPID1. See Table 3-13 for problems that can cause a particular line status.

Table 3-13. BRI Line Status

Status	Meaning	Next Best Step
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 the switch-type 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.

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 should match the ISDN signaling that the public carrier institutes on the line, which depends on its software, not necessarily on the switch's manufacturer.

View the Status of the Modem Interface. To check the status and configuration of the modem interface, enter:

Syntax: show interfaces modem <*slot*>/<*port*>

If the module is ready to provide backup, the status report should read "modem 1/2 is UP" and the line status should be "on-hook."

Troubleshooting a Modem Interface. The modem interface will not go up unless it is configured for the correct country. You must enter the modem code from the global configuration mode context. See "Setting the Country" on page 3-54.

Viewing Information about Demand Routing and Troubleshooting Problems

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 3-14 lists the **show** commands for demand routing.

Table 3-14. show Commands for Demand Routing

Command	Description
show interfaces 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 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 3-23 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**

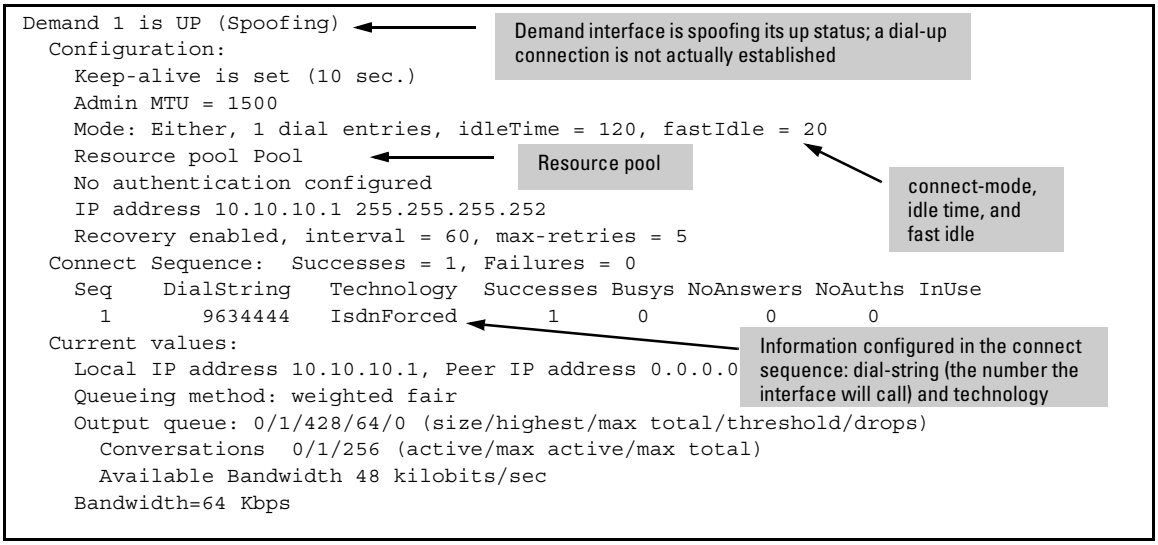

Figure 3-23. Viewing the Status of the Demand Interface When a Dial-Up Connection Has Not Been Established

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 idle timer)
- 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 3-24 provides the results of the **show interfaces demand 1** command when an ISDN connection has been established.

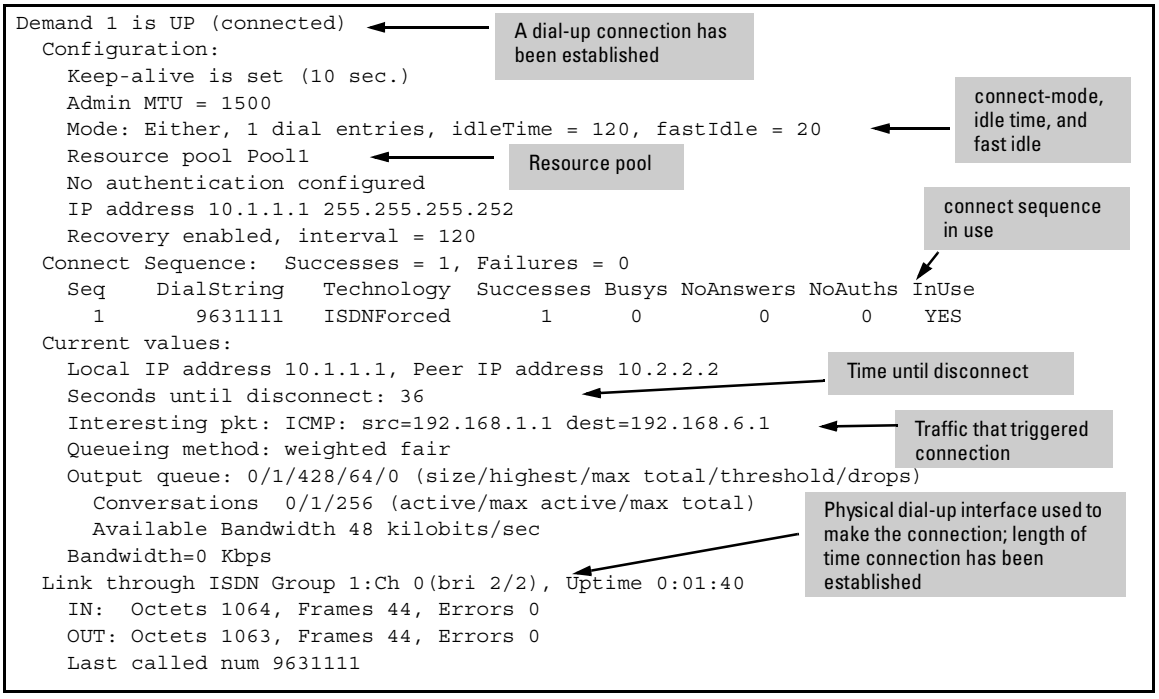

Figure 3-24. Viewing the Status of the Demand Interface When an ISDN Connection Is Established

Viewing a Summary of Information about the Demand Interface

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

Syntax: show demand interface 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

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 3-25.) 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

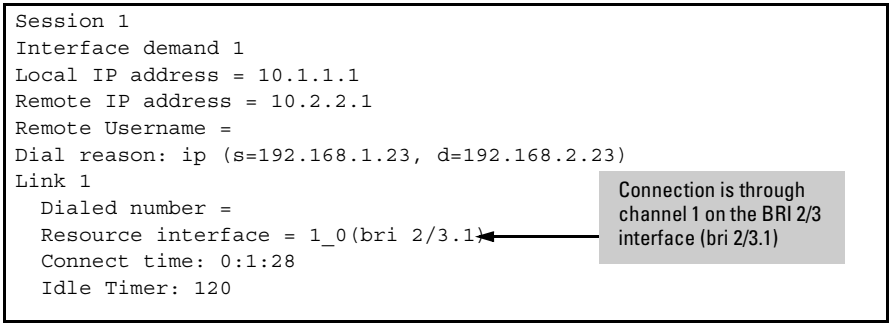

Figure 3-25. Viewing Demand Sessions

Viewing the Resource Pool

You can view which interfaces have been assigned to a particular resource pool. You can also view which demand interfaces use the pool. (See Figure 3-26.) From the enable mode context, enter:

ProCurve# show demand resource pool <*poolname*>

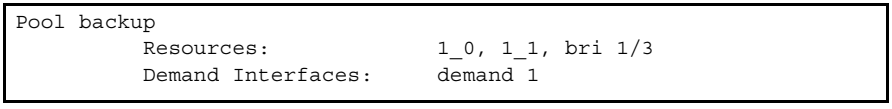

Figure 3-26. Viewing a Resource Pool

Show the Running-Config for the Demand Interface

To check your demand routing configuration, you must view the 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 3-27 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
  username procurve password procurve
  ppp pap sent-username procurve password procurve
  no shutdown
```

Figure 3-27. 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 backup 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 is up, has a valid IP address and connect sequence. You should also ensure that the associated BRI or modem interfaces are ready to

make a connection. (For more information about checking the BRI or modem interfaces, see "Viewing Information about BRI and Modem Interfaces and Troubleshooting Problems" on page 3-72.)

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). If this happens, the demand interface will remain down until you take corrective actions. You should first identify and fix the problem causing the failure. You can then change the status of the demand interface by disabling it and then activating it.

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

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

You can then activate the interface by entering:

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

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. If possible, disconnect the primary WAN connection so that the floating static route that you created for demand routing is listed in the routing table. View the routing table by entering the following command from the enable mode context:

```
ProCurve# show ip route
```

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.

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 Backup Connection

If the interesting traffic triggers the backup 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 you can use to troubleshoot ISDN backup connections. These commands are listed in Table 3-15.

Table 3-15. 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

Command	Description
debug isdn resource-manager	displays resource manager errors and messages
debug isdn verbose	display all errors and messages

Note Debug functions are processor intensive.

Some of the **debug isdn** commands display a high volume of messages, which are displayed too quickly to read. For example, Figure 3-28 shows a small portion of the debug messages displayed as a call connects. If you check the timestamp for these messages, you get an idea of how quickly the messages are being displayed to the CLI.

```
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
```

Figure 3-28. Viewing ISDN debug Messages

Test Calls for ISDN Lines

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 connect only at the Physical Layer.

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 2/3)# 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 2/3)# 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 2/3)# test-call hangup channels 1,2

or

ProCurve(config-bri 2/3)# 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 2/3)# 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.

Troubleshooting PPP for a Demand Routing Backup 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 3-16 lists the **debug** commands you can use to monitor PPP sessions.

Table 3-16. 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 negotiation	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

Viewing Information about Persistent Backup Connections and Troubleshooting Problems

When you are troubleshooting a persistent backup connection, you should verify the following:

- The backup dial list for the primary connection contains the remote router's number.
- Backup is enabled for the proper days and times.
- The backup interface has an IP address on a different network from the primary interface.
- If using authentication, the backup interface includes the correct username and password to send or to accept from a peer.

To verify this information, you can use the **show** commands in Table 3-17.

Table 3-17. Backup show Commands

View	Command Syntax
backup dial list	**show backup interfaces**
days and times backup is enabled	**show backup interfaces**
backup PPP interface IP address	• **show interfaces ppp <backup interface number>** • **show running-config interface ppp <backup interface number>**
backup PPP interface authentication information	**show running-config interface ppp <backup interface number>**

Viewing Backup Settings

To view the backup settings that are specific to each connection, enter this command:

```
ProCurve# show backup interfaces
```

The CLI will display a report on every logical interface for which backup is enabled. (See Figure 3-29.)

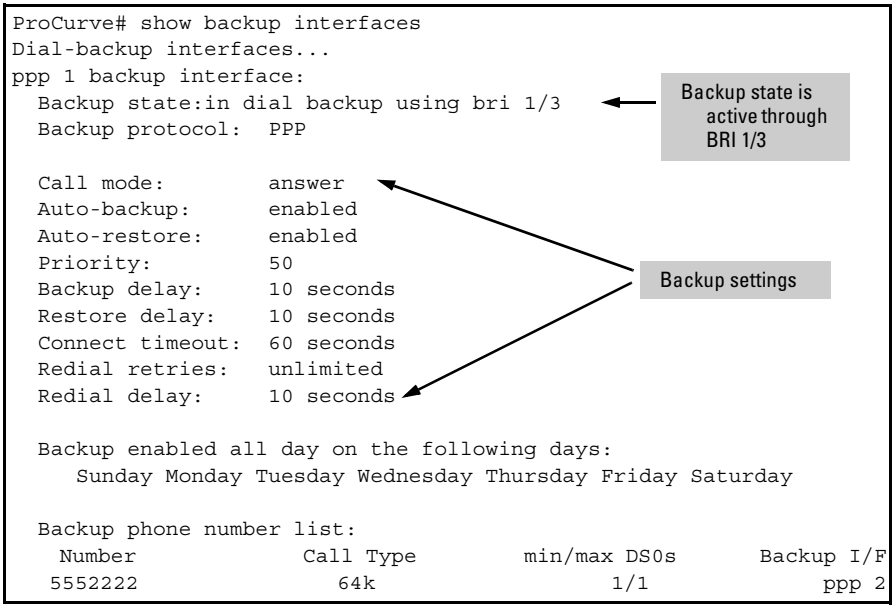

Figure 3-29. Viewing Backup Interfaces

For each interface, the report includes:

- Backup state—If the backup state is "idle," the primary connection is up. If the state is, for example, "in dial backup using..." the backup connection is active. The dial-up interface (bri 1/3, in the example above) indicates which backup line is active. Any available dial-up interface can provide the backup connection.
- Backup protocol—This is always PPP.
- Backup settings—Pay most attention to the interface's call mode, which determines its role in the backup call process. This role may be to originate calls, answer them, or both. This setting also indicates whether the interface can receive calls only during primary line failure or at any time (always). If you are having problems with a seemingly good line going down, an **always** setting can be to blame. The router could be answering a backup call and forcing the line down.

  This section of the report also shows parameters such as the delay between call attempts and the delay between line failure and backup initialization.
- Backup enabled—Backup is enabled for the times and days listed. Verify that these times are in keeping with your organization's policies.

- Backup phone number list—This is the backup dial list, which includes:
  - Number—the peer's phone number
  - Call type—analog, digital 56K, or digital 64K
  - Min/max DS0s—for ISDN lines only; the setting should read "1 2" for bonded lines
  - Backup I/F—the PPP interface that manages the backup connection

Note

You cannot view a logical interface's settings for persistent backup in the usual status report generated with the **show interfaces** command. You *must* enter **show backup interfaces**. The **show backup interfaces** command does *not* show backup PPP interfaces (which you view with the typical **show interfaces ppp *<interface number>*** command). Rather, it shows *backup settings* for *primary* logical interfaces.

Viewing the Backup PPP Interface

You can use the **show interfaces** command to view the IP address on the PPP interface for the persistent backup connection. However, this command will not show you all the authentication configurations. You should instead examine the running-config for the backup interface. For example:

```
ProCurve# show run int ppp 2
```

Monitoring the Dial-Up Process

Monitoring the dial-up process can help you discover why a backup connection does not come up when the primary connection fails. Use the **debug** commands to receive real-time messages about backup link negotiation:

```
ProCurve# debug backup
ProCurve# debug dialup-interfaces
```

The CLI displays backup messages received on both the dial-up and the logical interfaces. Messages appear marked with the date, time, type of event, and associated interface. For example:

```
2003.08.13 02:55:31 DIAL_BACKUP.bri 1/3
```

When the local router successfully connects to a peer, you should receive messages such as those shown in Figure 3-30.

```
ProCurve# debug backup
ProCurve# debug dialup-interfaces
DIALUP_INTERFACE.bri 1/3 Dialing 8882222
DIALUP_INTERFACE.bri 1/3 Connect (CONNECT 64000)
DIAL_BACKUP.bri 1/3 establishing ppp 1 backup to 8882222.
DIAL_BACKUP.bri 1/3 Backup connection up.
DIAL_BACKUP.ppp 1 Backup connection established to 8882222
```

Figure 3-30. Successfully Establishing a Backup Connection

The interface numbers and backup telephone number will, of course, be specific to your WAN.

If you receive the following message instead, you should follow the trouble-shooting procedure for calls that do not connect:

DIAL_BACKUP.Connect failed

See "The Call Does Not Connect" on page 3-92 to learn how to resolve specific problems that cause the connection to fail.

When the local router answers a backup call from a peer, you should receive messages such as those in figure 3-31.

```
ProCurve# debug backup
ProCurve# debug dialup-interfaces
2005.07.11 12:54:03 DIAL_BACKUP.bri 1/3 Answering call...
2005.07.11 12:54:08 DIALUP_INTERFACE.bri 1/3 Answering incoming call
2005.07.11 12:54:11 DIALUP_INTERFACE.bri 1/3 Connect (CONNECT 64000)
2005.07.11 12:54:11 DIAL_BACKUP.bri 1/3 Backup connection up.
2005.07.11 12:54:11 DIAL_BACKUP.ppp 1 Backup connection established
to 5552222
2005.07.11 12:54:11 DIAL_BACKUP.ppp 1 ppp 2
2005.07.11 12:54:22 PPP.NEGOTIATION bri 1/3: LCP up
2005.07.11 12:54:23 INTERFACE_STATUS.ppp 2 changed state to up
2005.07.11 12:54:24 PPP.NEGOTIATION LLDPCP up
2005.07.11 12:54:25 PPP.NEGOTIATION IPCP up
```

Figure 3-31. Answering a Call

The router will not answer a call if the number is not in its dial backup list. The router will receive a message such as this:

DIAL_BACKUP.MGR: Ignoring incoming call on bri 1/3 from 0005552222 because no match was found for this call source.

Troubleshooting Persistent Backup Connections

Monitoring the backup connection can point you in the general direction for troubleshooting. If the router does not establish a backup connection, examine the debug messages for clues to whether the interface is dialing a number but not connecting, or not dialing a number at all.

After the call connects, the router should receive PPP.NEGOTIATION messages through the BRI interface bringing the link up. If the dialup interface connects the call, but the backup PPP interface does not come up, you may have a problem with authentication.

Standard Procedures

You should monitor the backup call to determine the problem. Does the backup interface place a call at all? Does the call connect? Move to the section that describes your problem and follow the process described.

The BRI or Modem Interface Does Not Dial A Number. If no debug messages appear, then the backup interface is not dialing a number at all. Follow these steps:

1. View the BRI or modem interface (**show *<interface ID>***).
2. If the interface is down, troubleshoot the interface. (See "Troubleshooting a BRI Interface" on page 3-75 or "Troubleshooting a Modem Interface" on page 3-76.)
3. If the BRI or modem interface is up, the router, for some reason, cannot request backup for the failed connection.
4. If the modem interface is up, but does not establish a backup connection, it may be configured to support dialin console sessions. Disable this option if you want the modem to provide backup. If the **dialin** option is not enabled, proceed to the next step to look for another problem.
5. Enter **show backup int** and view the primary interface call mode. (See "Viewing Backup Settings" on page 3-87.)

6. If the call mode does not include **originate**, the router must wait to receive a call from the other end of the line. Either contact the remote site and have it initiate a connection or change the setting so the local router can place a call.
7. If the call mode includes **originate**, verify that backup is enabled at this time.
8. If backup is enabled, check the backup dial list (also displayed with **show backup int**). This list may be blank if, for example, you have changed a Frame Relay subinterface's Data Link Connection Identifier (DLCI).
9. If the dial backup list does not contain at least one number and backup interface, configure the list. Make sure that the number is that for the *remote* site.
10. If the dial backup list has been configured, note the backup interface specified in the dial backup list. View the status or running-config for this interface (**show int ppp 2** or **show run int ppp 2**) and verify that the interface has been configured and activated.

The Call Does Not Connect. See Table 3-18 for a summary of possible causes for a call failing to connect.

Table 3-18. Connect Failed Messages

Message	Possible Problems
Connect failed (BUSY)	• • The number configured in the backup dial list is not the peer's correct number. • The backup call has collided with the peer's call. • The peer refuses to or cannot answer the call.
Connect failed (Urgent Failure)	There is a problem between the local interface and the CO's switch.
Connect failed	The number configured in the backup dial list is not a valid number.

When a call from the local router to the peer fails, follow these steps:

1. A "Connect failed (BUSY)" often indicates a problem at the other end of the connection. The peer's backup interface may by down. The peer may also be rejecting your call. Contact the remote site and find the problem. You should also double-check that the telephone number on the local router's backup interface matches that accepted by the peer router.

In a PPP connection, when one end loses the connection the other does as well. If both endpoints are allowed to place a backup call, the calls may collide. In this situation, you may want to configure one router to answer calls and one to receive them. (See "Setting the Backup Call Mode" on page 3-61.)

You can also randomize backup timers to minimize the chance that the local backup call will collide with a call from the peer router. (See "Setting Backup Timers" on page 3-68.)

Finally, the router could be calling the wrong number. See step 2 for troubleshooting this problem.

2. If you simply receive a "Connect failed" message, the router may not be calling a valid number. Enter **show backup int** and view the backup dial list for the connection. (See "Viewing Backup Settings" on page 3-87.) Verify that the number is the *remote site's* correct number. You configure the local site's number in the BRI interface configuration mode. If the backup dial list includes the local number, the router will receive a "BUSY" message.

   Sometimes the Secure Router OS may delete a stored backup number—for example, if you change a Frame Relay interface's DLCI. If necessary, reenter the number.

3. If the number is correct, but the call still will not connect, increase the connect-timeout interval. This timer determines how long the router will wait for a call to connect before terminating the attempt. It should be at least 60 seconds. (See "Setting Backup Timers" on page 3-68.)

The Router Will Not Answer the Peer's Call. You may receive a debug message telling you that the router is ignoring a call because no match was found for the call. Follow these steps:

1. Enter **show backup int** and view the backup dial list for the connection. (See "Viewing Backup Settings" on page 3-87.)

2. Verify that the number is the peer's correct number. If necessary, remove a faulty number and add the correct one.

When the router will not answer a call and does not receive any debug messages, its own primary connection may still be up. For example, in a Frame Relay network, one site's connection may go down, while the other's connection to its Frame Relay provider is still good. Check the primary interface (or Frame Relay subinterface). If it is up, try changing its backup call mode to **answer-always** or **originate-answer-always**. This will allow the local router to establish the backup connection with the remote router.

The Call Connects But the Backup Connection Does Not Go Up.

Caution

These instructions explain how you can view PPP debug messages to determine why the Data Link Layer will not go up. However, if a PPP connection is currently up, these debug messages can swamp the router and seriously degrade network performance. It can be safer to simply double-check PPP authentication settings.

Even if the backup connection is the router's only PPP connection, you should be very careful with PPP **debug** commands.

Follow these steps:

1. You can view PPP debug messages to determine why the Data Link Layer will not go up. Enter **debug ppp verbose**.
2. Look particularly for PPP.AUTHENTICATION messages.
3. Determine whether the local or the remote router cannot authenticate itself. For CHAP, look for a Challenge message; for PAP, look for an Authen-Nak. The peer that sends this message is the host that requires its peer to authenticate itself. (See "Troubleshooting PPP Authentication" on page 6-63 in the *Basic Management and Configuration Guide* for more information on interpreting these debug messages.)
4. If authentication does not seem to be the problem, scan PPP debug messages for other problems. See troubleshooting tips for PPP in "Troubleshooting the PPP Interface" on page 6-59 in the *Basic Management and Configuration Guide*.
5. If the *remote router* requires the local router to authenticate itself, view the running-config for the backup PPP interface (**show run int ppp *<interface number>***) and verify that the interface is configured to send the correct username and password. It must also be using the correct type of authentication.

   The username and password the router sends is listed under **ppp pap sent-username** or **ppp chap hostname** and/or **ppp chap password**.

   The router automatically sends its hostname for the CHAP password. If necessary, override this hostname with the correct username. (See "Enabling PPP Authentication" on page 3-58.)

6. If the *local router* requires the remote router to authenticate itself, view the running-config for the backup PPP interface (**show run int ppp *<interface number>***) and verify that the interface contains the correct username and password for the peer.

   The username and password the router accepts are listed under **username** and **password**. Remember that these might be different than those in the local database configured from the global configuration mode context.

7. Turn off the debug messages by entering **undebug all**.

The Backup Connection Goes Up But Traffic Does Not Reach Its Destination. Follow these steps:

1. View the route table (**show ip route**). The table should now include a route to the remote network(s) that either lists the backup interface as the forwarding interface or the peer's backup interface IP address as the next hop address.
2. If necessary, add a static route to the remote network.
3. If you are using dynamic routing, verify that you have enabled the protocol on the backup network. If you are using BGP to advertise local networks, the BGP interface should be able to advertise the backup network.

The Backup Connection Goes Up When the Primary Connection Is Still Good. This problem can be caused in two ways:

- The primary interface is configured to always answer backup calls—If the connection to the router placing the backup call is most important, this is not necessarily a problem. However, if this setting has been configured in error, you must change the backup call mode for the primary connection. (See "Setting the Backup Call Mode" on page 3-61.)
- The backup interface has been configured with backup settings—It is very important to configure all backup settings, including the backup dial list and backup call mode, on the *primary* interface. If, for example, you enter a backup number in backup PPP interface 2, the router will consider it to be a primary connection. It will notice that the PPP 2 is down, so it will initiate a backup call.

The Router Does Not Call the Secondary Number When the First Call Does Not Connect. You can add more than one number to a primary interface's backup dial list. If, when the router attempts to initiate a backup call, the call to the first number does not connect, the router calls the second number.

However, by default, the number of times the router reattempts to connect a call is set to unlimited. The router will continue to try the first number rather than moving on to the second.

Whenever you want the router to be able to contact more than one number for a backup connection, you should limit the number of times the router can attempt a call. Enter this command from the logical interface for the primary connection:

Syntax: backup maximum-retry <*attempts*>

For example:

```
ProCurve(config-ppp 1)# backup maximum retry 3
```

Quick Start

You have two choices for configuring how the ProCurve Secure Router responds to a backup condition:

- You can configure demand routing, which is enabled if a primary interface goes down and traffic must be transmitted to the far-end network. The backup connection only remains active for as long as this traffic must be transmitted.
- You can configure a persistent backup connection, which is initiated immediately if a primary connection goes down and stays up until the primary connection is available again.

This section provides the commands you must enter to quickly configure either types of backup connection using:

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

Only a minimal explanation is provided. If you need additional information about any of these options, check “Contents” on page 3-1 to locate the section that contains the explanation you need.

Configuring Demand Routing for Backup Connections

You may want to use Table 3-19 to record the information you will need to configure demand routing for a backup module.

Table 3-19. Settings for Configuring Demand Routing for a Backup Module

Required Configuration	Options	Your Setting
Define the traffic that should initiate the dial-up connection if the primary interface is down. You need the source and destination addresses for this traffic.	Permit and deny statements in the ACL: **[permit | deny] <protocol> <source address> <source port> <destination address> <destination port>**	
Create a demand interface.	Specify a number between 1 and 1024: **interface demand <number>**	
Specify the IP address for the demand interface.	Different network address than the address assigned to the primary connection	
Specify the number to call to reach far-end network, the type of backup interface to use, and number of times to try calling the number.	• Far-end network's LDN • Resource types: – **forced-analog** – **isdn-56k** – **isdn-65k** – **forced-isdn-56k** – **forced-isdn-65k** • Busyout threshold: 1 to 65535	
Specify whether the router can place a call, answer a call, or both.	• **originate** • **answer** • **either**	
Access the configuration mode context for the backup interface.	**<backup interface> = bri** or **modem** **<slot> = 1** or **2** **<port> = 2** or **3**	
For an analog interface, specify the country in which the router is located.	Enter **modem country code ?** for a complete list of codes. (Enter this command from the global configuration mode context.)	
For ISDN connections, specify the ISDN signaling that the service provider implements on the line.	• National ISDN-1= **basic-ni** • Euro ISDN = **basic-net3** • Northern Telecom DMS-100 = **basic-dms** • Lucent/ATT 5ESS = **basic-5ess**	
For ISDN connections in North America, specify the service profile ID (SPID).	Obtained from service provider	

Required Configuration	Options	Your Setting
For ISDN connections, specify the LDN, the local telephone number for the ISDN line.	Obtained from service provider	
Create a floating static route to the far-end network.	• Obtain the destination network address from the remote site • Administrative distance should be higher than that for the primary route	
Define the number of seconds that the connection should remain up if no interesting traffic is received. You should base this setting on the billing interval for your company's ISDN line.	1 to 2147483 seconds	
Create a resource pool that contains the BRI and modem interfaces that demand routing can use to establish backup connections	Alphanumeric name	

After recording the information for your WAN, complete these steps:

1. Enter the global configuration mode context.

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

2. Create an extended 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 extended ACL configuration mode context, configure permit or deny entries. Enter:

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

Replace ***<protocol>*** with one of the following:

- **ahp**
- **esp**
- **gre**
- **icmp**
- **ip**
- **tcp**
- **udp**
- number between 0 and 255

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

Syntax: [any | host <*A.B.C.D*> |hostname <*hostname*> | <*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 Backup ACL to demand 1 interface, enter:

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

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 site
   – the type of dial-up connection to establish

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

Syntax: connect-sequence <*sequence-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 LDN that the demand interface should dial to make the connection.

Replace ***<resource-type>*** with one of the options listed in Table 3-20. The option you enter will limit this connection to a particular type of dial-up connection.

Replace ***<value>*** with the number of times between 1 and 65535 that the demand interface should attempt the call. (Enter **0** to have the demand interface make an unlimited number of attempts.)

Table 3-20. Defining a Resource Type for Connection Instructions

Option	Description
isdn-64k	Any dial resource can be used, but if ISDN is used, the call must be placed using 64 KB.
isdn-56k	Any dial resource can be used, but if ISDN is used, the call must be placed using 56 KB.
forced-analog	Only analog resources can be used.
forced-isdn-64k	Only ISDN resources can be used, and the call must be placed using 64 KB.
forced-isdn-56k	Only ISDN resources can be used, and the call must be placed using 56 KB.

f. The idle timer determines the length of time the backup connection can be idle before the demand interface terminates it. If so desired, you can set the timer to match the billing increments for your backup connection. Enter this command from the demand interface configuration mode context:

Syntax: idle-timeout <1-2147483>

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 1/2

   b. Set the ISDN signaling (switch) type if your service provider is not using the default setting for the ISDN module your are using. 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 (switch) type, enter:

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

Table 3-21 lists the command syntax for each signaling type.

Table 3-21. 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. 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. Make the BRI interface a member of the resource group:

Syntax: resource pool-member <*poolname*>

For example, if you want to assign the BRI interface to a resource pool called “backup,” enter:

```
ProCurve(config-bri 1/1)# resource pool-member Backup
```

f. Activate the interface. Enter:

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

5. Create a floating static route to the far-end network. The route should use the demand interface as the forwarding interface. From the global configuration mode context, enter:

Syntax: ip route <*destination A.B.C.D*> <*subnet mask* | /*prefix length*> demand <*number*> [<*administrative distance*>]

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. Specify the forwarding interface as **demand *<number>*** and include an administrative distance that is higher than the administrative distance for the route through the primary interface.

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

```
ProCurve(config)# ip route 192.168.7.0 /24 demand 1 2
```

Configuring a Persistent Backup Connection

To help you keep track of the information you need to enter when configuring a persistent backup connection, you can print and complete Table 3-22.

Table 3-22. Backup Settings

Required Configuration	Options	Your Setting
Access the configuration mode context for the backup interface.	**<backup interface> = bri** or **modem** **<slot> = 1** or **2** **<port> = 2** or **3**	
For an analog interface, specify the country in which the router is located.	Enter **modem country code ?** for a complete list of codes. (Enter this command from the global configuration mode context.)	
For ISDN connections, specify the ISDN signaling that the service provider implements on the line.	• National ISDN-1= **basic-ni** • Euro ISDN = **basic-net3** • Northern Telecom DMS-100 = **basic-dms** • Lucent/ATT 5ESS = **basic-5ess**	
For ISDN connections in North America, specify the service profile ID (SPID).	Obtained from service provider	
For ISDN connections, specify the LDN, the local telephone number for the ISDN line.	Obtained from service provider	
Create a backup PPP interface.	Specify a number between 1 and 1024: **interface ppp <number>**	
Specify an IP address for a backup PPP interface.	Different network address than the address assigned to the primary connection	
Specify the number to call to reach far-end network.	Obtained from remote site	
Determine whether the router can place or answer backup calls, or both.	• **originate** • **answer** • **answer-always** (answer backup calls even when the local connection is good) • **originate-answer** (default) • **originate-answer-always**	

Required Configuration	Options	Your Setting
Specify days that backup will *not* be provided.	• **sunday** • **monday** • **tuesday** • **wednesday** • **thursday** • **friday** • **saturday**	
Specify time when backup support is turned off.	hh:mm:ss For example, **18:30:00**	
Specify time when backup support is turned back on.	hh:mm:ss For example, **8:45:00**	
Create a floating static route to the far-end network.	• Obtain the destination network address from the remote site • Administrative distance should be higher than that for the primary route	

1. Install the backup module. Refer to the "Installation Instructions" in the *ProCurve Secure Router dl ISDN BRI U Backup Module Quick Start Guide*.
2. Power up the router and move to the global configuration mode context. Enter the BRI configuration mode context.

   Syntax: interface bri <*slot*>/<*port*>
3. Enter the ISDN signaling type.

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

   For example:

   ProCurve(config-bri 1/3)# isdn switch-type basic-ni
4. Enter the SPID and LDN.

   Syntax: isdn spid1 <*SPID1*> <*local site's LDN*>
5. If you are using both B channels, you may need to enter a second SPID and LDN.

   Syntax: isdn spid2 <*SPID2*> <*local site's LDN 2*>
6. Activate the interface.

   ProCurve(config-bri 1/3)# no shutdown

7. Create a backup PPP interface.

   Syntax: interface ppp <*backup interface number*>

8. Assign the backup interface a static IP address on a different network than the primary interface.

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

9. Activate the interface.

   ProCurve(config-ppp 2)# no shutdown

10. Move to the logical interface for the primary connection.

    Syntax: interface <*interface ID*>

    For example:

    ProCurve(config)# interface frame-relay 1.102

11. Add the *remote site's* telephone number to the backup call list.

    Syntax: backup number <*remote site's LDN*> [digital-56k | digital-64k] [1 1 | 1 2] ppp <*backup interface number*>

    Use **1 1** for a single channel and **1 2** for a bonded channel. For example:

    ProCurve(config-fr 1.102)# backup number 5552222 digital-64k 1 2 ppp 2

Note

Bonding calls is a ProCurve proprietary technology, so you can only place a bonded call to another ProCurve Secure Router.

12. Set the backup call mode.

    Syntax: backup call-mode [originate | answer | answer-always | originate-answer | originate-answer-always]

    For example, the router connects to the remote site through a Frame Relay network. The connection on one side might still be up when the other goes down, so you set the call mode to **originate-answer-always**.

    ProCurve(config-fr 1.102)# backup call-mode originate-answer-always

13. Disable backup for the days and times you do not want to provide backup.

    Syntax: no backup schedule day <*day*>
    Syntax: backup schedule disable-time <*hh:mm:ss*>
    Syntax: backup schedule enable-time <*hh:mm:ss*>

    Enter times in twenty-four hour clock format. For example:

    ```
    ProCurve(config-fr 1.102)# no backup schedule saturday
    ProCurve(config-fr 1.102)# backup schedule disable-time 18:00:00
    ProCurve(config-fr 1.102)# backup schedule enable-time 8:00:00
    ```

14. If you are using static routing, add a floating static route to the remote site. From the global configuration mode context, enter:

    Syntax: ip route <*remote network A.B.C.D*> [<*subnet mask*> | /<*prefix length*>] [<*remote backup A.B.C.D*> | ppp <*backup interface number*>] [<administrative distance>]

    Set the administrative distance higher than the route through the primary connection so that the router will only add the backup route to its table if the primary connection fails. For example, enter:

    ```
    ProCurve(config)# ip route 192.168.3.0 /24 ppp 2 2
    ```

Backing up a Connection with an ISDN BRI S/T Backup Module

1. Install the backup module. Refer to the "Installation Instructions" in the *ProCurve Secure Router dl ISDN BRI S/T Backup Module Quick Start Guide*.
2. Power up the router and move to the global configuration mode context. Enter the BRI interface configuration mode context.

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

3. Enter the ISDN signaling type.

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

    For example:

    ```
    ProCurve(config-bri 1/3)# isdn switch-type basic-net3
    ```

4. Enter the LDN.

    Syntax: isdn ldn1 <*local site's LDN*>

5. If necessary, enter a second LDN.

    Syntax: isdn ldn2 <*local site's LDN* 2>

6. Activate the interface.

   ProCurve(config-bri 1/3)# no shutdown

7. Create a backup PPP interface.

   Syntax: interface ppp <*backup interface number*>

8. Assign the backup interface an IP address on a different network than the primary interface.

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

9. Activate the interface.

   ProCurve(config-ppp 2)# no shutdown

10. Move to the logical interface for the primary connection.

    Syntax: interface <*interface ID*>

    For example:

    ProCurve(config)# interface frame-relay 1.102

11. Add the *remote site's* telephone number to the backup call list.

    Syntax: backup number <*remote site's LDN*> [digital-56k | digital-64k] [1 1 | 1 2] ppp <*backup interface number*>

    Use **1 1** for a single channel and **1 2** for a bonded channel. For example:

    ProCurve(config-fr 1.102)# backup number 5552222 digital-64k 1 2 ppp 2

Note

Bonding calls is a ProCurve proprietary technology, so you can only place a bonded call to another ProCurve Secure Router.

12. Set the backup call mode.

    Syntax: backup call-mode [originate | answer | answer-always | originate-answer | originate-answer-always]

    For example, the router connects to the remote site through a Frame Relay network. The connection on one side might still be up when the other goes down, so you set the call mode to **originate-answer-always**.

    ProCurve(config-fr 1.102)# backup call-mode originate-answer-always

13. Disable backup for the days and times you do not want to provide backup.

    Syntax: no backup schedule day <*day*>
    Syntax: backup schedule disable-time <*hh:mm:ss*>
    Syntax: backup schedule enable-time <*hh:mm:ss*>

    Enter times in 24-hour clock format. For example:

    ```
    ProCurve(config-fr 1.102)# no backup schedule saturday
    ProCurve(config-fr 1.102)# backup schedule disable-time 18:00:00
    ProCurve(config-fr 1.102)# backup schedule enable-time 8:00:00
    ```

14. If you are using static routing, add a floating static route to the remote site.

    Syntax: ip route <*remote network A.B.C.D*> [<*remote subnet mask*> | /<*prefix length*>] [<*remote backup A.B.C.D*> | ppp <*backup interface number*>] [<administrative distance>]

    Set the administrative distance higher than the route through the primary connection so that the router will only add the backup route to its table if the primary connection fails. For example, enter:

    ```
    ProCurve(config)# ip route 192.168.3.0 /24 ppp 2 2
    ```

Backing up a Connection with an Analog Module

1. Install the backup module. Refer to the "Installation Instructions" in the *ProCurve Secure Router dl Analog Backup Module Quick Start Guide*.
2. Power up the router and move to the global configuration mode context. If the router is in any country except the USA or Canada, specify the country. (Use the **?** help command to get a list of the keywords for countries.)

   Syntax: modem countrycode <*country*>
3. Enter the modem interface configuration mode context.

   Syntax: interface modem <*slot*>/<*port*>
4. Activate the interface.

   ```
   ProCurve(config-modem 1/3)# no shutdown
   ```
5. Create a backup PPP interface.

   Syntax: interface ppp <*backup interface number*>
6. Assign the backup interface an IP address on a different network than the primary interface.

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

7. Activate the interface.

   ProCurve(config-ppp 2)# no shutdown

8. Move to the logical interface for the primary connection.

   Syntax: interface <*interface ID*>

   For example:

   ProCurve(config)# interface frame-relay 1.102

9. Add the *remote site's* telephone number to the backup call list.

   Syntax: backup number <*remote site's LDN*> analog ppp <*backup interface number*>

   For example:

   ProCurve(config-fr 1.102)# backup number 5552222 analog ppp 2

10. Set the backup call mode.

    Syntax: backup call-mode [originate | answer | answer-always | originate-answer | originate-answer-always]

    For example, the router connects to the remote site through a Frame Relay network. The connection on one side might still be up when the other goes down, so you set the call mode to **originate answer always**.

    ProCurve(config-fr 1.102)# backup call-mode originate-answer-always

11. Disable backup for the days and times you do not want to provide backup.

    Syntax: no backup schedule day <*day*>
    Syntax: backup schedule disable-time <*hh:mm:ss*>
    Syntax: backup schedule enable-time <*hh:mm:ss*>

    Enter times in 24-hour clock format. For example:

    ProCurve(config-fr 1.102)# no backup schedule saturday
    ProCurve(config-fr 1.102)# backup schedule disable-time 18:00:00
    ProCurve(config-fr 1.102)# backup schedule enable-time 8:00:00

12. If you are using static routing, add a floating static route to the remote site.

    Syntax: ip route <*remote network A.B.C.D*> [<*remote subnet mask*> | /<*prefix length*>] [<*remote backup A.B.C.D*> | ppp <*backup interface number*>] [<administrative distance>]

    Set the administrative distance higher than the route through the primary connection so that the router will only add the backup route to its table if the primary connection fails. For example, enter:

    ProCurve(config)# ip route 192.168.3.0 /24 ppp 2 2