Designing ISDN Internetworks

Integrated Services Digital Network (ISDN) services are becoming more prevalent in networking and communications. More network administrators are turning to ISDN to solve a variety of wide-area networking connectivity problems. In particular, ISDN is rapidly gaining acceptance for telecommuting applications.

ISDN involves the digitization of the telephone network so that voice, data, text, graphics, music, video, and other source material can be provided to end users from a single terminal over existing telephone wiring. In the future, ISDN may be deployed in a worldwide network much like the present telephone network, with digital transmission serving as the foundation for services such as video conferencing and high-speed imaging (Group IV facsimile) and file transfer.

For general information about ISDN devices, services, layers, and frame formats, as well as the sequence of messages that establishes an ISDN call, see the *Internetworking Technology Overview* publication.

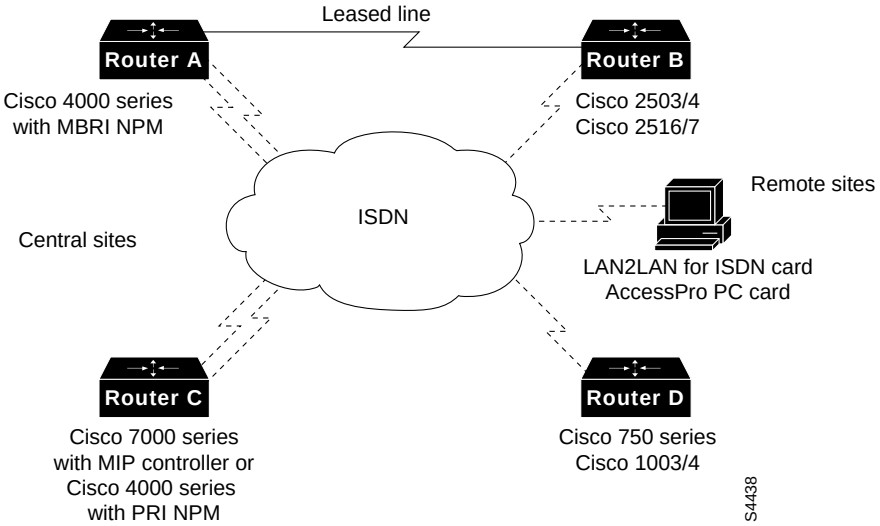
Introduction

A variety of different network design options take advantage of both ISDN Basic Rate Interface (BRI) and Primary Rate Interface (PRI) services. Typically, a remote site with a single BRI dials a central site equipped with multiple BRIs, a single PRI, or multiple PRIs.

ISDN can also be used as a backup service for a leased-line connection between the remote and central offices. If the primary link (T1, fractional T1, E1, or fractional E1) goes down, an ISDN circuit-switched connection is established and traffic is rerouted over ISDN. When the primary link is restored, traffic is redirected to the leased line, and the ISDN link is torn down. ISDN dial backup can also be configured based on traffic thresholds on the primary link. If traffic load exceeds a user-defined value on the primary link, the ISDN link is activated to increase bandwidth between the two sites.

The topology shown in Figure 11-1 includes all of the Cisco routers that can be configured for ISDN. In Figure 11-1, Router A and Router C are located in central offices and are equipped with multiple ISDN interfaces for use by the remote sites (Router B and Router D) that dial in.

Figure 11-1 ISDN Network Topology



Remote Site Options

The remote site can be a Cisco 750, a LAN2LAN for ISDN card, an AccessPro PC card, a Cisco 1003/4, a Cisco 2503/4, or a Cisco 2516/7.

The Cisco 750 series (formerly Combinet) provides ISDN connectivity for telecommuters and professionals who work at home that need IP and IPX routing or bridging functionality over ISDN. The Cisco 751 supports up to four devices on the directly attached LAN. The Cisco 752 also supports four devices and includes a built-in NT1. The Cisco 753 supports four devices, includes a built-in NT1, and includes an analog interface that allows a standard analog telephone, fax machine, or modem to share the ISDN BRI line with data traffic, reducing the overall cost of the telecommuting solution. Unlike the other products described in this chapter, the Cisco 750 series routers do not run the Cisco Internetwork Operating System (Cisco IOS) software, so the commands and configuration examples in this chapter do not apply to the Cisco 750 series.

The LAN2LAN for ISDN card is suitable for telecommuters and professionals who work at home that already have a PC. The card can be installed in the ISA or EISA slot of a PC chassis and is available in single BRI (requires one slot) and four-port BRI (requires two slots) configurations. The card comes with an Open Data-link Interface (ODI) workstation driver. LAN2LAN for ISDN supports IP and IPX routing and bridging over ISDN connections, with special software features to allow automatic dial-on-demand routing (DDR), bandwidth on demand, maintenance of virtual host-client connections, and data compression. The LAN2LAN card is configured through a menu interface, so the commands and configurations examples in this chapter do not apply to this card.

The AccessPro PC card is suitable for small remote offices that already have a PC. The card can be installed in the ISA or EISA slot of a PC chassis and provides one ISDN BRI, two synchronous serial ports, and either one Ethernet interface or one Token Ring interface. The AccessPro runs the Cisco IOS software and does not rely on the PC for route processing—all routing functionality resides on the card itself, so the AccessPro card does not affect the performance of other applications that may

be running on the PC. These features make the Cisco AccessPro PC card suitable for small businesses and home offices that have a small Ethernet or Token Ring network whose users occasionally need to connect to a central site.

The Cisco 1003 is a desktop router that, with one BRI and one Ethernet interface, provides connectivity for small-to-medium size remote offices. It runs the Cisco IOS software, which routes IP, IPX, and AppleTalk and bridges other protocols. The Cisco 1004 is similar to the Cisco 1003, but it contains a built-in NT1.

The Cisco 2503 is suitable for medium-to-large size remote offices. It provides one Ethernet interface, one BRI, and two synchronous serial ports. The Cisco 2504 provides one Token Ring interface, one BRI, and two synchronous serial ports for connectivity over leased lines.

The Cisco 2516 is suitable for large remote offices. It provides one Ethernet interface (14 hub ports), two synchronous serial ports, and one BRI. The Cisco 2517 provides one Token Ring interface (11 hub ports), one BRI, and two synchronous serial ports for connectivity over leased lines.

Central Site Options

The central site can be a Cisco 4000 series router, which supports up to 16 BRIs provided by network processor module cards (NPMs). The Cisco 4000 series can also be configured with up to two multichannel interface processor (MIP) cards. Each MIP card provides two PRIs. The T1 version of the MIP card yields 23 B channels and one 64-kbps D channel per MIP card interface. The E1 version of the MIP card yields 30 B channels and one 64-kbps D channel.

The central site can also be a Cisco 7000 series router or a Cisco 7500 series router with MIP cards providing PRIs.

Table 11-1 summarizes the ISDN capabilities of Cisco routers.

Table 11-1 Cisco Routers ISDN Support

Router Product	ISDN Interface
Cisco 750 series	One BRI
AccessPro PC card	One BRI
Cisco 1003/4	One BRI
Cisco 2503/4	One BRI
Cisco 2516/17	One BRI
Cisco 4000 series router (per NPM)	Four or eight BRIs per NPM, one PRI per NPM
Cisco 7000 series/Cisco 7500 series	One or two PRIs per MIP

Central Office Considerations

When designing your ISDN network, you need to consider the central office switches through which your ISDN connections will be made. Telephone companies use a variety of central office switches, each with unique characteristics that affect the way in which you configure your router equipment. This section discusses the following characteristics of central office switches:

- Switch Type
- TEI Negotiation (BRI only)
- Service Profile Identifiers (SPIDs) (BRI only)
- Signaling System 7
- ISDN Interfaces
- Calling Line Identification

Switch Type

Some manufacturers of ISDN central office switches (also known as *local exchange equipment*) divide the local exchange into two functions: local termination and exchange termination. The local termination function primarily deals with the transmission facility and termination of the local loop. The exchange termination function deals with the switching portion of the local exchange. First, the exchange termination function demultiplexes the bits on the B and D channels. Next, B channel information is routed to the first stage of the circuit switch, and D-channel packets are routed to D-channel packet separation circuitry.

Several companies manufacture ISDN-compatible central office switches. Today, the AT&T 5ESS and the NorTel DMS-100 are the two principal ISDN switches in North America. Until the current release of National ISDN-1 software, incompatibility between the AT&T and NorTel switches meant, for example, that AT&T ISDN telephone sets could not be used with a NorTel switch.

The 5ESS was introduced in 1982 and can provide up to 100,000 local loops. Approximately 1600 5ESS switches are in use worldwide, serving close to 40 million lines. In the United States, over 85 percent of the BRI lines in service terminate at a 5ESS-equipped central office.

The NorTel DMS-100 switch family is intended to deliver a wide range of telecommunication services. The DMS-100, introduced in 1978, can terminate up to 100,000 lines. The DMS-10 is a smaller version of the DMS-100 and supports up to 10,800 lines. The DMS-200 is intended for switching offices in the toll network, equal-access end offices, or access tandem switch applications. The DMS-250 is a toll switch for specialized common carriers requiring tandem switch operation. The DMS-300 is intended for international gateway operations.

Although AT&T and NorTel have deployed the most ISDN switches, there are other ISDN switch manufacturers. Table 11-2 lists the ISDN-capable switches that are used in Australia, Europe, Japan, and New Zealand, where ISDN switches are country specific. The Keyword column lists the keyword that is used with the **isdn switch-type** command to configure the router for the type of switch that the router connects to. Your telephone company can tell you the type of switch that is located in the central office to which your router will connect.

Table 11-2 ISDN Switches in Australia, Europe, Japan, and New Zealand

Country	Switch Type	Keyword
Australia	TS013 BRI switch, TS014 PRI switch	basic-ts013, primary-ts014
France	VN2 ISDN switch, VN3 ISDN switch	vn2, vn3
Germany	1TR6 ISDN switch	basic-1tr6
Japan	NTT ISDN switch, ISDN PRI switch	ntt, primary-ntt
New Zealand	NET3 ISDN switch	basic-nznet3
Norway	NET3 ISDN switch (phase 1 only)	basic-nwnet3
United Kingdom	NET3 BRI switch, NET5 PRI switch	basic-net3, primary-net5

Table 11-3 lists the ISDN-capable switches that are used in Canada and the United States.

Table 11-3 ISDN Switches in Canada and the United States

Switch Type	Keyword
AT&T basic rate switch	basic-5ess
NorTel DMS-100 basic rate switch	basic-dms100
National ISDN-1 switch	basic-ni1
AT&T 4ESS (ISDN PRI only)	primary-4ess
AT&T 5ESS (ISDN PRI only)	primary-5ess
NorTel DMS-100 (ISDN PRI only)	primary-dms100

Note The functionality of the National ISDN switch is evolving. The levels of functionality are known as NI1, NI2, and NI3.

TEI Negotiation

(This section applies to BRIs only.) Some switches deactivate Layer 2 of the D channel when no calls are active, so the router must be configured to perform TEI negotiation at the first call instead of at router power-up (the default).

Service Profile Identifiers

(This section applies to BRIs only.) A service profile identifier (SPID) is a number provided by the ISDN carrier to identify the line configuration of the BRI service. SPIDs allow multiple ISDN devices, such as voice and data, to share the local loop. SPIDs are required by DMS-100 and National ISDN-1 switches. Depending on the software version it runs, an AT&T 5ESS switch might require SPIDs.

Each SPID points to line setup and configuration information. When a device attempts to connect to the ISDN network, it performs a D-channel Layer 2 initialization process that causes a TEI to be assigned to the device. The device then attempts D-channel Layer 3 initialization. If SPIDs are necessary but not configured on the device, the Layer 3 initialization fails, and the call cannot be completed.

The AT&T 5ESS switch supports up to eight SPIDs per BRI. Because multiple SPIDs can be applied to a single B channel, multiple services can be supported simultaneously. For example, the first B channel can be configured for data, and the second B channel can be configured for both voice (using an ISDN telephone) and data.

DMS-100 and National ISDN-1 switches support only two SPIDs per BRI—one SPID for each B channel. If both B channels will be used for data only, configure the router for both SPIDs (one for each B channel). You cannot run data and voice over the same B channel simultaneously. The absence or presence of a channel's SPID in the router's configuration dictates whether the second B channel can be used for data or voice.

Note There is no standard format for SPID numbers. As a result, SPID numbers vary depending on the switch vendor and the carrier.

The **isdn spid1** and **isdn spid2** interface configuration commands are used to assign SPID values for a given BRI. These commands also allow the specification of the local directory number (LDN), which is a seven-digit number assigned by the service provider that is part of the incoming setup message. The LDN is not necessary for establishing ISDN-based connections, but it must be specified if you want to receive incoming calls on B channel 2. The LDN is required only when two SPIDs are configured (for example, when connecting to a DMS or NI1 switch). Each SPID is associated with an LDN. Configuring the LDN causes incoming calls to B channel 2 to be answered properly. If the LDN is not configured, incoming calls to B channel 2 will fail.

Signaling System 7

In the United States, Signaling System 7 allows central office switches to communicate with other central office switches at 64 kbps. Some central office switches in the United States have not been upgraded to Signaling System 7, so they transfer data at 56 kbps. If your ISDN connection includes a central office switch that does not use Signaling System 7, configure the router configured with **dialer map** commands that place the call at 56 kbps. You also need to apply the **bandwidth** interface configuration command to the ISDN interface to notify routing protocols that the line operates at 56 kbps.

Incoming Call Delivery

When originating calls are made at 56 kbps but delivered to the destination by the ISDN network at 64 kbps, the incoming data can be corrupted. However, on ISDN calls, if the router is informed that the call is not ISDN end-to-end, it can set the line speed for the incoming call. This information is delivered in the incoming ISDN setup message.

To set the speed for incoming calls recognized as not ISDN end-to-end, use the **isdn not-end-to-end** interface configuration command to set the line speed at which calls are answered.

Calling Line Identification

Some central office switches support calling line identification (known as *caller ID*), which allows the router to verify that an incoming call comes from an expected source. If your router connects to a central office switch that supports caller ID, you can configure the router to match the caller ID delivered as part of the call setup against a configured value. If the values do not match, the router rejects the call. For more information about this ISDN security feature, see the "Screening" section later in this chapter.

ISDN Interfaces

ISDN provides multiple data channels—two B channels for BRI service (2B+D), 23 B channels for T1 PRI (23B+D), or 30 B channels for E1 PRI (30B+D). This section describes the way Cisco products identify ISDN interfaces.

Basic Rate Interface

The ISDN BRI provides 2 B channels for sending and receiving data at 64 kbps, and 1 D channel for signaling or communicating with the ISDN switch at 16 kbps. The two B channels are automatically placed in a rotary group. On ISDN dialers configured for X.25 encapsulation (Cisco IOS Software Release 10.2), however, only one B channel can be used.

Cisco has received certification for ISDN BRI compliance for the countries listed in Table 11-4.

Table 11-4 Certification for ISDN BRI Compliance

Australia	Germany	Spain
Austria	Ireland	Sweden
Belgium	Japan	Switzerland
Canada	New Zealand	The Netherlands
Denmark	Norway	United Kingdom
Finland	Portugal	United States

On the AccessPro PC card, the BRI interface is identified by “interface B0.”

On the Cisco 1003/4, 2503/4, and 2516/17 routers, the ISDN BRI is identified by “interface bri 0.” On the Cisco 4000 series router, the ISDN interfaces are numbered 0 through 3 (for the four-port MBRI) and 0 through 7 (for the eight-port MBRI.) If two four-port MBRIs are installed, the interfaces are numbered from 1 through 8, and if two eight-port MBRIs are installed, the interfaces are numbered 1 through 16.

PRIs

The ISDN PRI for the United States, Canada, and Japan provides 23 B channels and one D channel (all at 64 kbps) for a cumulative speed equivalent to T1 (1.5 Mbps). The B channels are automatically placed in a rotary group. ISDN for Europe provides 30 B channels and one D channel (all at 64 kbps) for a cumulative speed equivalent to E1 (2 Mbps). ISDN PRI is supported with Cisco IOS Software Release 10.2 for 5ESS, 4ESS, and DMS-100 in North America.

In the United States, the T1 MIP card provides PRIs on Cisco 4000 or Cisco 7000 series routers. To configure a MIP card, use the **controller** global configuration command. The **controller** command specifies the type of interface (T1 or E1), the slot in which the MIP card is installed, and the port that is being configured. Then use the **framing** and **linecode** controller configuration commands to specify the framing type and the line code type, which are required for T1 and E1 connections.

To specify that the MIP card is to be used as an ISDN PRI, use the **pri-group** controller configuration command. If only a portion of the channels are to be used for ISDN, use the **timeslots** keyword and specify the range of channels that is to be used for ISDN.

For T1 PRI, when the **timeslots** keyword is not specified, the **pri-group** command defaults to 23 B channels with one D channel, with channels 1 through 23 as B channels and channel 24 for the D channel. The **pri-group** command creates a logical interface called "interface serial *slot-number-of MIP card* /*port-number*:23." You use this interface to configure network protocol information and DDR information that applies to all the channels of the PRI.

Note For T1 PRI, B channel 1 corresponds to logical serial 0, and D channel 24 corresponds to logical serial 23.

The following commands configure a T1 controller positioned in port 0 of slot 2 as an ISDN PRI using the Extended Super Frame frame type and the Bipolar 8 Zero Substitution line code type:

```
controller t1 2/0
framing esf
linecode b8zs
pri-group
interface serial 2/0:23
```

An E1 version of the MIP card can be used as an ISDN PRI for I.421 Euro-ISDN signaling when used with the ISDN PRI signaling software available in Cisco IOS Software Release 10.3 or later.

The following commands configure an E1 controller positioned in port 1 of slot 1 as an ISDN PRI using the CRC4 frame type and the High-Density Bipolar 3 line code type:

```
controller e1 1/1
framing crc4
linecode hdb3
pri-group

interface serial 1/1:15
!Interface configuration commands go here.
```

When the **pri-group** command does not specify the **timeslots** keyword, the E1 controller defaults to 30 B channels and one D channel, with channels 1 through 15 and 17 through 31 as B channels and channel 16 for the D channel. The command creates a logical interface called "interface serial *slot-number-of MIP card* /*port-number*:15." You use this interface to configure network protocol information and DDR information that applies to all the channels of the PRI.

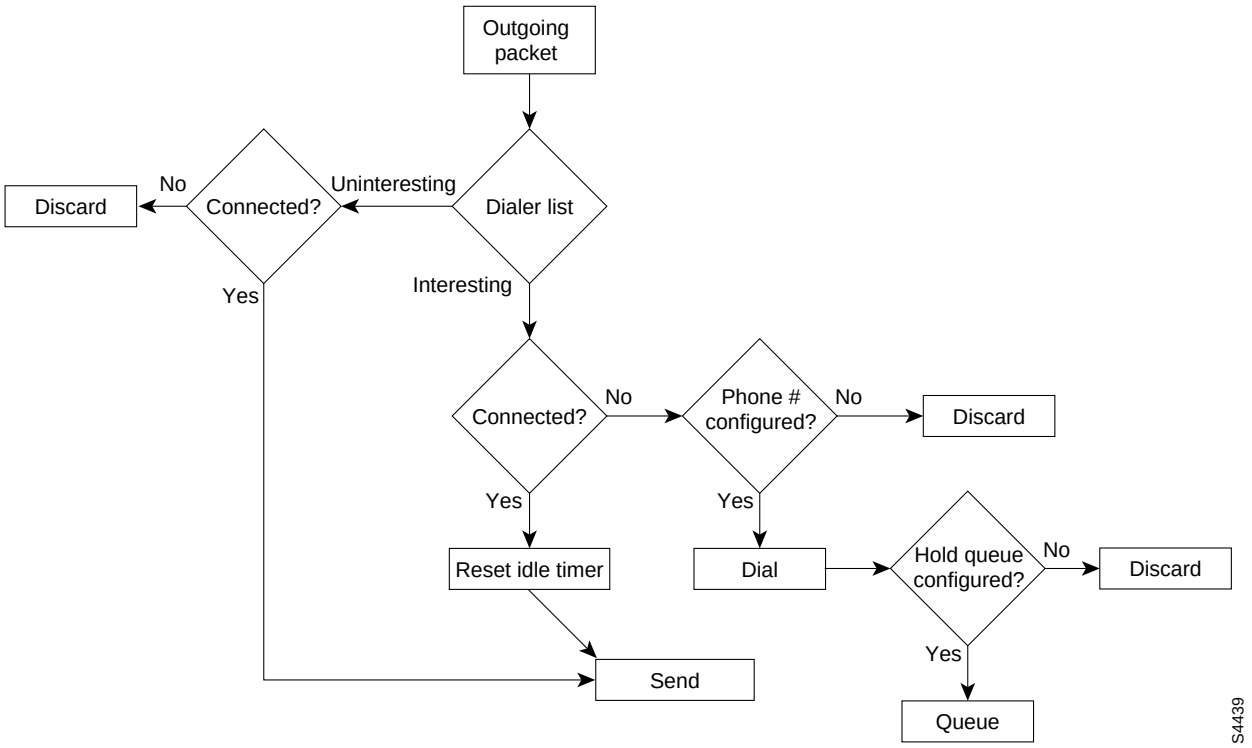
Note For E1 PRI, B channel 1 corresponds to serial 0, and D channel 16 corresponds to serial 15.

In Australia, the TS014 PRI switch uses channel 16 as the D channel and channels 1 through 15 and 17 through 30 as B channels.

Dial-on-Demand Routing

ISDN is a circuit-switched technology. Like the analog telephone network, ISDN connections are made only when there is a need to communicate. Cisco uses dial-on-demand routing (DDR) to determine when a connection needs to be made between two sites. With DDR, packets are classified as either *interesting* or *uninteresting* based on protocol-specific access lists and dialer lists. DDR makes an ISDN connection only if the packet is interesting. Figure 11-2 shows the DDR decision process for determining packet flow of an ISDN connection.

Figure 11-2 DDR Flow Chart



In Figure 11-2, an outgoing packet is compared with the configured dialer lists. If the packet is found to be *interesting* and a connection is already established for the destination, the router resets the idle timer and sends the packet. If the packet is found to be interesting but a connection to the destination is not active, the router checks to see if a phone number is configured for the destination. If a phone number is configured, the router dials the destination and sends the packet.

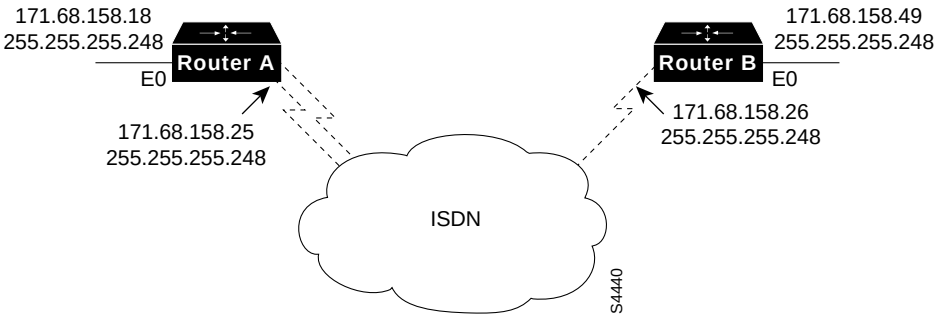
When dealing with ISDN, it is important to consider cost structures. Typically, the initiator of an ISDN connection incurs a cost each time a connection is made and for each minute that the connection remains in effect. The primary goal of router configuration is to minimize the number of connections and the duration of connections without sacrificing end-user connectivity.

This chapter summarizes information about DDR as it pertains to ISDN. For detailed information about designing internetworks for use with DDR, see the chapter, “Designing DDR Internetworks.”

Configuring IP DDR over ISDN

In Figure 11-3, Router A dials Router B and Router B dials Router A over ISDN by means of IP DDR.

Figure 11-3 Sample IP ISDN Topology



IP Addressing

Use the **ip address** command to assign an IP address to the ISDN interface. The ISDN interface of both routers must be on the subnet. Alternatively, you can use the **ip unnumbered interface** command instead of the **ip address** command. The **ip unnumbered interface** command allows the ISDN interface to the IP address of a LAN interface as its own.

IP Routing

IP routing between sites can be handled by static routes or a routing protocol such as Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Enhanced IGRP, or Open Shortest Path First (OSPF). Because they send regular update packets, routing protocols are usually ill-suited for ISDN networks because they initiate costly connections solely for the purpose of sending update packets. If you are using RIP or IGRP, you can control update packets by using snapshot routing. (For a discussion of snapshot routing, see the “Snapshot Routing” section later in this chapter.

To configure static routes, use the **ip route** global configuration command. The **ip route** command maps IP hosts and networks to an intermediate address. The configuration for the remote router (Router B) maps all destinations available at the central site to the central site BRI port’s address (the intermediate address).

Note If the central site is running a routing protocol, the central site router must use the **redistribute** router configuration command with the **static** keyword to redistribute the static routes for the remote site.

IP Dialer Lists

The **dialer-list list** global configuration command defines interesting packets. A dialer list can permit or deny Layer 3 traffic or it can call a more specific Layer 2 or Layer 3 access list. The following **dialer-list** command is a generic statement that creates dialer list 5 and permits all IP traffic:

```
dialer-list 5 protocol ip permit
```

The following **dialer-list** command creates dialer list 3 and calls all extended access lists numbered 101:

```
dialer-list protocol ip 3 list 101
access-list 101 permit ip any any
access-list 101 deny udp any any eq snmp
```

The **access-list** global configuration command establishes access lists, which use network-layer filtering to control traffic. Standard IP access lists are numbered from 1 to 99 and extended access lists are numbered between 100 and 199. Both types of access list can be called by a **dialer-list** command.

To associate a dialer list with a specific ISDN interface, use the **dialer-group** interface configuration command.

IP Dialer Maps

The **dialer map** interface configuration command associates a network address with an ISDN number. In addition to specifying the IP address of the destination router and the ISDN number to be dialed, the **dialer map** command specifies the name of the router that is being called (which must match the name of the router to pass authentication) and the speed at which the call is to be placed.

Note The name that is used in the **dialer map** statement must also exist as a user name with a password on the router that is being dialed.

The following is an example of the **dialer map** command:

```
dialer map ip 171.68.158.25 name RouterA broadcast 1408555111
```

The **broadcast** keyword permits broadcast traffic to cross the ISDN link in addition to the regular unicast traffic that is permitted. If static routes are used, the **broadcast** keyword is not necessary. If RIP or IGRP is used, however, the **broadcast** keyword is necessary so that routing updates can cross the link. You can use a combination of snapshot routing and access lists to prevent connections from being established for the sole purpose of exchanging protocol updates. See the “Tariff Management” section later in this chapter.

If the ISDN interfaces are configured using the **ip unnumbered** command, the **dialer map** command should specify the IP address that is used in the **ip unnumbered** command for the ISDN interface on the router that is being dialed.

Encapsulation and Authentication

ISDN interfaces can be configured for High-Level Data Link Control (HDLC), Frame Relay, Link Access Procedure, Balanced (LAPB), Point-to-Point Protocol (PPP), and X.25 encapsulation. When you configure PPP encapsulation, you can specify the use of Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). CHAP is recommended because it sends an encrypted form of the password. (PAP sends the password in clear text.)

Sample IP Configuration

The following configurations for Router A and Router B use DDR to enable IP over BRI 0 using static IP routes. For information about using access lists to prevent routing updates from initiating connections, see the section "Tariff Management" later in this chapter.

```
hostname RouterA
!
enable password ######
!
username RouterB password 7 2394943E02B17
isdn switch-type basic-5ess
!
interface ethernet 0
ip address 171.68.158.18 255.255.255.248
!
interface bri 0
ip address 171.68.158.25 255.255.255.248
encapsulation ppp
dialer map ip 171.68.158.26 name RouterB 14085552222
dialer-group 1
ppp authentication chap
!
ip route 171.68.158.48 255.255.255.248 171.68.158.26
access-list 101 permit ip any any
!
dialer-list 1 protocol ip list 101
```

The configuration for Router B is as follows:

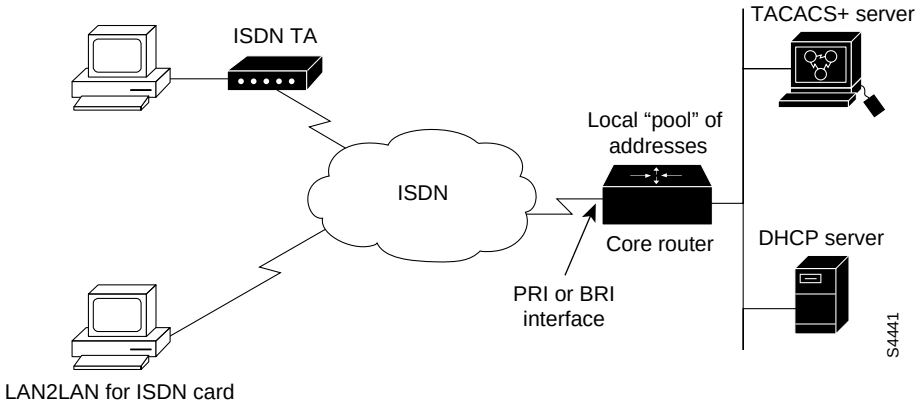
```
!hostname RouterB
!
enable password ######
!
username RouterA password 7 094E5B1739522
isdn switch-type basic-5ess
interface ethernet 0
ip address 171.68.158.49 255.255.255.248
!
interface bri 0
ip address 171.68.158.26 255.255.255.248
encapsulation ppp
dialer map ip 171.68.158.25 name RouterA 14085551111
dialer-group 1
ppp authentication chap
!
ip route 171.68.158.16 255.255.255.248 171.68.158.25
access-list 101 permit ip any any
!
dialer-list 1 protocol ip list 101
```

IP Address Negotiation for ISDN

IP address negotiation allows remote node PPP client software to request an IP address from a Cisco core router during call setup. This request is part of the PPP IP Control Protocol (IPCP) setup negotiation. IP address negotiation is specifically designed for remote node connectivity where the end user uses a PC workstation with a nonrouting device, such as a Cisco LAN2LAN for ISDN card, or an external ISDN terminal adapter.

The core router can assign IP addresses from a local *pool* maintained by the core router or from a Terminal Access Controller Access Control System Plus (TACACS+) server or a Dynamic Host Configuration Protocol (DHCP) server, as shown in Figure 11-4.

Figure 11-4 IP Address Negotiation



Note The core router can be configured to assign addresses from more than one type of pool. For example, the core router can be configured to obtain addresses from the local pool for certain dial-up users and to obtain addresses from the TACACS+ server for other dial-up users.

IP address negotiation allows an organization to manage its address space centrally and to minimize address utilization. With IP address negotiation, you need to provide only enough address space to cope with worst case loading scenarios. Use of IP address negotiation also reduces configuration text in the core router. Because of the dynamic nature of IP address assignment, the core router no longer needs to maintain a specific dialer map statement for each remote node. IP address negotiation creates dynamic dialer maps for each individual connection and removes them at the end of the session.

Note It is important to ensure that addresses are negotiated via PPP IPCP. Some client software stacks support DHCP locally. If the remote node originates the DHCP request, the core router cannot function as a DHCP proxy, so a return path will not be available through the core router.

Local Address Assignment

The core router can be configured to maintain several pools of IP addresses, with each pool holding up to 255 addresses. Each pool has a free queue containing available addresses and a "used" queue containing addresses that are currently in use. On receipt of the IPCP address negotiation request, the core router retrieves an address from the free queue. The client can request the same address that was used for the last connection. If this address is in the free queue, it is assigned. If the requested address is in use, another address from the free queue is assigned.

TACACS+ Address Assignment

The TACACS+ server can be configured to assign the remote node's IP address after it authorizes the remote node's connection or it can be configured to return to the core router the name of a local address pool from which the core router obtains an IP address that it assigns to the remote node.

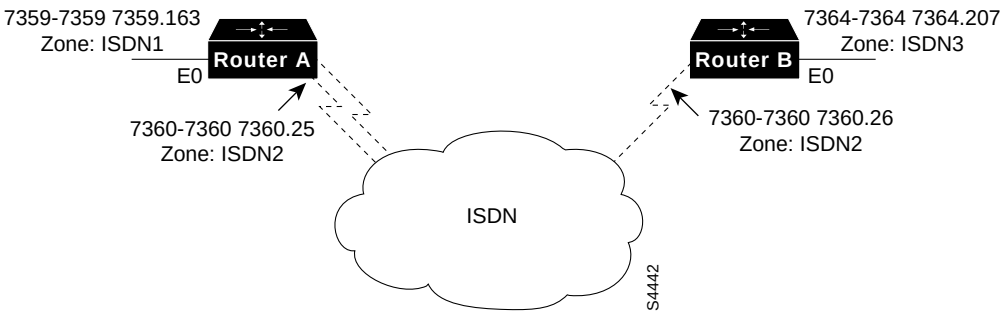
DHCP

When using DHCP, the core router acts as a DHCP proxy for the remote node. On receipt of the IPCP address negotiation request, the core router retrieves an IP address from the DHCP server. At the end of the session, the router returns the address to the server. The router can also act as a DHCP relay agent.

Configuring AppleTalk DDR over ISDN

In Figure 11-5, Router A dials Router B and Router B dials Router A over ISDN using AppleTalk DDR.

Figure 11-5 Sample AppleTalk over ISDN Topology



AppleTalk Addressing

The **appletalk cable-range** interface configuration command specifies the cable-range and node address of each ISDN interface. The cable range must be the same on both ends of the connection. The **appletalk zone** interface configuration command must be entered on both routers. Use the same zone name on both routers' ISDN interfaces. The remote LAN interface, however, should have a different zone name to reduce AppleTalk broadcasts across the link, as shown in Figure 11-5.

AppleTalk Routing

Use the **appletalk routing** global configuration command to enable AppleTalk routing. The default AppleTalk routing protocol is RTMP, with AppleTalk Enhanced IGRP Enhanced IGRP as an option. Because AppleTalk Enhanced IGRP sends out a "hello" packet every 5 seconds, RTMP is better suited to networks that connect by means of ISDN.

AppleTalk Dialer Lists

AppleTalk dialer lists are similar to IP dialer lists. They can be used in two ways: to establish general protocol access or to call more specific access lists. The following **dialer-list** command is a generic statement that creates dialer list 2 and permits all AppleTalk traffic:

```
dialer-list 2 protocol AppleTalk permit
```

The following **dialer-list** command creates dialer list 6 and calls all extended access lists numbered 601:

```
dialer-list 6 protocol appletalk list 601
access-list 601 deny cable-range 7364-7364
access-list 601 permit other-access
```

The **access-list** command establishes access lists, which use network-layer filtering to control traffic. AppleTalk access lists are numbered between 600 and 699. The **access-list cable-range** command denies the forwarding of AppleTalk packets from cable range 7364-7364. The **access-list other-access** command permits the forwarding of AppleTalk packets from any other cable range.

Some AppleTalk applications send out license management packets that, if not controlled, initiate unnecessary connections. AppleShare 4.0, for example, sends out license management packets to ensure that the same copy is not being run elsewhere. The license management packets are broadcast to each cable range, which inherently include ISDN links. An access list can make the license management packets *uninteresting* and prevent them from bringing up the link. The following commands create an access list that for cable range 7364-7364 makes broadcasts (including license management packets) *uninteresting* and all other traffic *interesting*:

```
access list 601 permit cable-range 7364-7364 broadcast-deny
access-list 601 deny other-access
```

To associate a dialer list with a specific ISDN interface, use the **dialer-group** interface configuration command.

Note Because only one **dialer-group** command is allowed per interface, all of the **dialer-list** commands associated with a specific interface must use the same number.

AppleTalk Dialer Maps

When used in AppleTalk networks, the **dialer map** interface configuration command associates an AppleTalk network address with an ISDN number. In addition to specifying the AppleTalk address of the destination router and the ISDN number to be dialed, the **dialer map** command specifies the name of the router that is being called (which, to pass PPP CHAP authentication, must match the name of the router) and the speed at which the call is to be placed. (Note that the name that is used in the **dialer map** statement must also exist as a user name with a password on the local router.) The following is an example of the **dialer map** command:

```
dialer map appletalk 7360.25 name RouterB broadcast 14085551212
```

The **broadcast** keyword allows AppleTalk routing updates to cross the ISDN link. If static routes are being used, the **broadcast** keyword is not necessary. You can use a combination of snapshot routing and access lists to prevent connections from being established for the sole purpose of exchanging protocol updates. See the “Tariff Management” section later in this chapter.

Sample AppleTalk Configuration

The following configurations for Router A and Router B use DDR to enable IP and AppleTalk over BRI 0. For information about using access lists to prevent routing updates from initiating connections, see the "Tariff Management" section later in this chapter.

```
hostname RouterA
!
enable password ######
!
username RouterB password 7 2394943E02B17
AppleTalk routing

isdn switch-type basic-5ess

interface ethernet 0
ip address 171.68.158.18 255.255.255.248
appletalk cable-range 7359-7359 7359.163
appletalk zone ISDN1
!
interface bri 0
ip address 171.68.158.25 255.255.255.248
encapsulation ppp
appletalk cable-range 7360-7360 7360.25
appletalk zone ISDN2
dialer map ip 171.68.158.26 name RouterB broadcast 14085552222
dialer map appletalk 7360.26 name RouterB broadcast 14085552222
dialer-group 1
ppp authentication chap
!
ip route 171.68.158.48 255.255.255.248 171.68.158.26
access-list 101 permit ip any any
!
dialer-list 1 protocol ip list 101
dialer-list 1 protocol appletalk permit
```

The configuration for Router B is as follows:

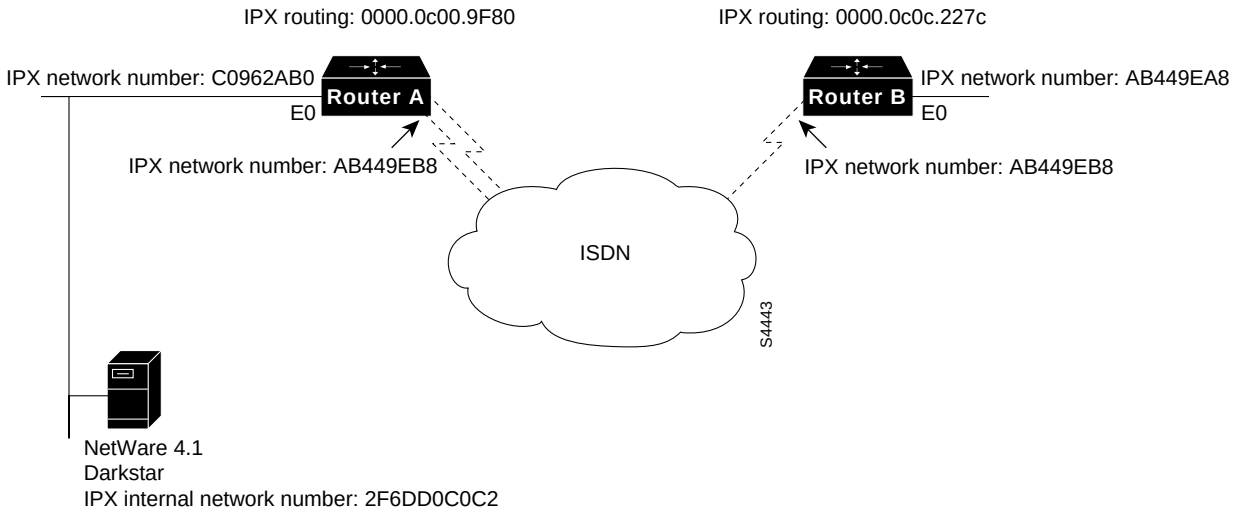
```
hostname RouterB
!
enable password ######
!
username RouterA password 7 094E5B1739522
AppleTalk routing
isdn switch-type basic-5ess

interface ethernet 0
ip address 171.68.158.49 255.255.255.248
AppleTalk cable-range 7364-7364 7364.207
AppleTalk zone ISDN3
!
interface bri 0
ip address 171.68.158.26 255.255.255.248
AppleTalk cable-range 7360-7360 7360.26
appletalk zone ISDN2
encapsulation ppp
dialer map ip 171.68.158.25 name RouterA speed 64 14085551111
dialer map AppleTalk 7360.25 name RouterA speed 64 broadcast 14085551111
dialer-group 1
ppp authentication chap
!
ip route 171.68.158.16 255.255.255.248 171.68.158.25
access-list 101 permit ip any any
!
dialer-list 1 protocol ip list 101
dialer-list 1 protocol AppleTalk permit
```

For information about optimizing AppleTalk connections over ISDN, see the sections “Tariff Management” and “Performance,” later in this chapter.

Configuring IPX DDR over ISDN

In Figure 11-6, Router A connects to Router B and Router B connects to Router A over ISDN using IPX DDR.

Figure 11-6 Sample IPX over ISDN Topology



IPX Addressing

Use the **ipx network** interface configuration command to assign the same IPX network address to each ISDN interface. You can use the **ipx route** command to create static IPX routes. Creating static IPX routes is not necessary if a dynamic routing protocol, such as RIP/SAP or NLSP), is in use.

IPX Routing

The **ipx routing** global configuration command enables IPX routing on the router. The default IPX routing protocol is RIP/Service Advertisement Protocol (SAP). Routers running Cisco IOS Software Release 10.3 or later can configure NetWare Link Services Protocol (NLSP) instead of RIP/SAP. Although NLSP has its advantages, it might be preferable to run RIP/SAP over ISDN, because snapshot routing can control RIP/SAP updates and help to keep the ISDN link down. Snapshot routing does not support NLSP.

IPX Dialer Lists

IPX dialer lists are similar to IP dialer lists. They can be used in two ways: to establish general protocol access or to call more specific access lists. The following **dialer-list** command is a generic statement that creates dialer list 2 and permits all IPX traffic:

```
dialer-list 2 protocol ipx permit
```

The following **dialer-list** command creates dialer list 6 and calls all extended access lists numbered 901:

```
dialer-list 6 protocol ipx list 901
access-list 901 permit -1 -1
```

The **access-list** command establishes access lists, which use network-layer filtering to control traffic. Standard IPX access lists are numbered from 800 to 899 and extended access lists are numbered between 900 and 901. The first "-1" permits packets from any network, and the second "-1" permits packets destined to any network.

To associate a dialer list with a specific ISDN interface, use the **dialer-group** interface configuration command.

Note Because only one **dialer-group** command is allowed per interface, all of the **dialer-list** commands associated with a specific interface must use the same number.

IPX Dialer Maps

When used in IPX networks, the **dialer map** interface configuration command associates an IPX network address with an ISDN number. In addition to specifying the IPX address of the destination router and the ISDN number to be dialed, the **dialer map** command specifies the name of the router that is being called (which, to pass PPP CHAP authentication, must match the name of the router) and the speed at which the call is to be placed.

Note The name that is used in the **dialer map** statement must also exist as a user name with a password on the local router.

The following is an example of the **dialer map** command:

```
dialer map IPX AB449EB8.0000.0c00.9f80 name althea broadcast 14085551111
```

The **broadcast** command allows RIP and SAP routing updates to cross the ISDN link. If static routes are being used, the **broadcast** keyword is not necessary. You can use a combination of snapshot routing and access lists to prevent connections from being established for the sole purpose of exchanging protocol updates. See the "Tariff Management" section later in this chapter.

Sample IPX Configuration

The following configurations for Router A and Router B use DDR to enable IP, AppleTalk, and IPX over BRI 0. For information about using access lists to prevent routing updates from initiating connections, see the "Tariff Management" section later in this chapter.

```
hostname RouterA
!
enable password ######
!
username RouterB password 7 2394943E02B17
appletalk routing
ipx routing 0000.0c00.9F80
isdn switch-type basic-5ess

interface ethernet 0
ip address 171.68.158.18 255.255.255.248
ipx network C0962AB0
ipx encapsulation SAP
appletalk cable-range 7359-7359 7359.163
appletalk zone ISDN1
!
interface bri 0
ip address 171.68.158.25 255.255.255.248
ipx network AB449EB8
encapsulation ppp
appletalk cable-range 7360-7360 7360.25
appletalk zone ISDN2
dialer map ip 171.68.158.26 name RouterB speed 64 14085552222
dialer map appletalk 7360.26 name RouterB speed 64 broadcast 14085552222
dialer map IPX AB449EB8.0000.0c0c.227c name RouterB speed 64 broadcast 14085552222
dialer-group 1
ppp authentication chap
!
ip route 171.68.158.48 255.255.255.248 171.68.158.25
access-list 101 permit ip any any
!
dialer-list 1 protocol ip list 101
dialer-list 1 protocol appletalk permit
dialer-list 1 protocol novell permit
```

The configuration for Router B is as follows:

```
hostname RouterB
!
enable password ######
!
username RouterA password 7 094E5B1739522
appletalk routing
ipx routing 0000.0c0c.227c
isdn switch-type basic-5ess
!
interface ethernet 0
ip address 171.68.158.49 255.255.255.248
ipx network AB449EA8
ipx encapsulation SAP
appletalk cable-range 7364-7364 7364.207
appletalk zone ISDN3
!
interface bri 0
ip address 171.68.158.26 255.255.255.248
ipx network AB449EB8
encapsulation ppp
appletalk cable-range 7360-7360 7360.26
appletalk zone ISDN2
```

```
dialer map ip 171.68.158.25 name RouterA speed 64 14085551111
dialer map appletalk 7360.25 name RouterA speed 64 broadcast 14085551111
dialer map IPX AB449EB8.0000.0c00.9f80 name RouterA speed 64 broadcast 14085551111
dialer-group 1
ppp authentication chap
!
ip route 171.68.158.16 255.255.255.248 171.68.158.25
access-list 101 permit ip any any
!
! The next two commands are optional if dynamic routing is used.
ipx route 2FCB6448 AB449EB8.0000.0c00.9f80
ipx route AB449EA0 AB449EB8.0000.0c00.9f80
!
!The next command establishes a static SAP entry and is optional if
!dynamic routing is used.
!
ipx sap 4 DARKSTAR 2F6DD0C0C2.0000.0000.0001 451 2
!
dialer-list 1 protocol ip list 101
dialer-list 1 protocol AppleTalk permit
dialer-list 1 protocol novell permit
```

For information about optimizing IPX connections over ISDN, see the sections “Tariff Management” and “Performance,” later in this chapter.

IPX Floating Static Routes

With Cisco IOS Software Release 10.3 or later, the administrative distance of an IPX static route can be configured so that the static route is less desirable than a dynamic route. This technique is known as *floating static routes*. If the dynamic route is lost, the floating static route can take over, and traffic can be sent through this alternative route. When an ISDN interface is configured as a floating static route, it can be used as a backup mechanism.

Tariff Management

As a circuit-switched connection, ISDN is billed, or *tariffed*, based on usage. Given this model, the configuration goal is to minimize up time by controlling the kinds of packets that bring the link up. Minimizing up time becomes a challenge when routing protocols are used because of their need to send regular broadcasts that contain routing information.

This section describes the following techniques for controlling routing updates:

- Routing
- Access Lists
- Protocol-Specific Techniques

Depending on the protocols your network runs, you might want to use a combination of the techniques described in this section.

Routing

Routing protocols can generate traffic that causes connections to be made unnecessarily. The following techniques can be used to control routing protocol traffic:

- Static Routes
- Snapshot Routing

Static Routes

With static routes, all routes are entered manually, eliminating the need for a routing protocol to broadcast routing updates. Static routes can be effective in small networks that do not change often. However, static routes in large networks that change often can become an administrative burden. Be sure to use access lists to control other packets that the protocol might generate.

Snapshot Routing

With snapshot routing, the router is configured for dynamic routing; snapshot routing controls the update interval of the routing protocols. Snapshot routing works with the following distance vector protocols:

- Routing Information Protocol (RIP) for IP
- Interior Gateway Routing Protocol (IGRP) for IP
- Routing Information Protocol (RIP) and Service Advertisement Protocol (SAP) for Novell Internet Packet Exchange (IPX)
- Routing Table Maintenance Protocol (RTMP) for AppleTalk
- Routing Table Protocol (RTP) for Banyan VINES

Under normal circumstances, these routing protocols broadcast updates every 10 to 60 seconds, so an ISDN link would be made every 10 to 60 seconds simply to exchange routing information. From a cost perspective, this frequency is prohibitive. Snapshot routing solves this problem.

Note Snapshot routing is available in Cisco IOS Software Release 10.2 or later.

Snapshot Model

Snapshot routing uses the client-server design model. When snapshot routing is configured, one router is designated the snapshot server, and one or more routers are designated as snapshot clients. The server and clients exchange routing information during an active period. At the beginning of the active period, the client router dials the server router to exchange routing information. At the end of the active period, each router takes a snapshot of the entries in its routing table. These entries remain frozen during a quiet period. At the end of the quiet period, another active period begins, and the client router dials the server router to obtain the latest routing information. The client router determines the frequency at which it calls the server router. The quiet period can be as long as 100,000 minutes (approximately 69 days).

When the client router transitions from the quiet period to the active period, the line might be down or busy. If this happens, the router would have to wait through another entire quiet period before it could update its routing table, which might severely affect connectivity if the quiet period is very long. To avoid having to wait through the quiet period, snapshot routing supports a retry period. If the line is not available when the quiet period ends, the router waits for the amount of time specified by the retry period and then transitions to an active period.

The retry period is also useful in dial-up environments in which there are more remote sites than interface lines. For example, the central site might have one PRI (with 23 B channels available) but might dial more than 23 remote sites. In this situation, there are more **dialer map** commands than available lines. The router tries the dialer map commands in order and uses the retry time for the lines that it cannot immediately access.

Enabling Snapshot Routing

Snapshot routing is enabled through interface configuration commands. The central router is configured for snapshot routing by applying the **snapshot server** interface configuration command to its ISDN interfaces. The **snapshot server** command specifies the length of the active period and whether the router is allowed to dial remote sites to exchange routing updates in the absence of regular traffic.

The remote routers are configured for snapshot routing by applying the snapshot client command to each ISDN interface. The **snapshot client** interface configuration command specifies the length of the active period (which must match the length specified on the central router), the length of the quiet period, whether the router can dial the central router to exchange routing updates in the absence of regular traffic, and whether connections that are established to exchange user data can be used to exchange routing updates.

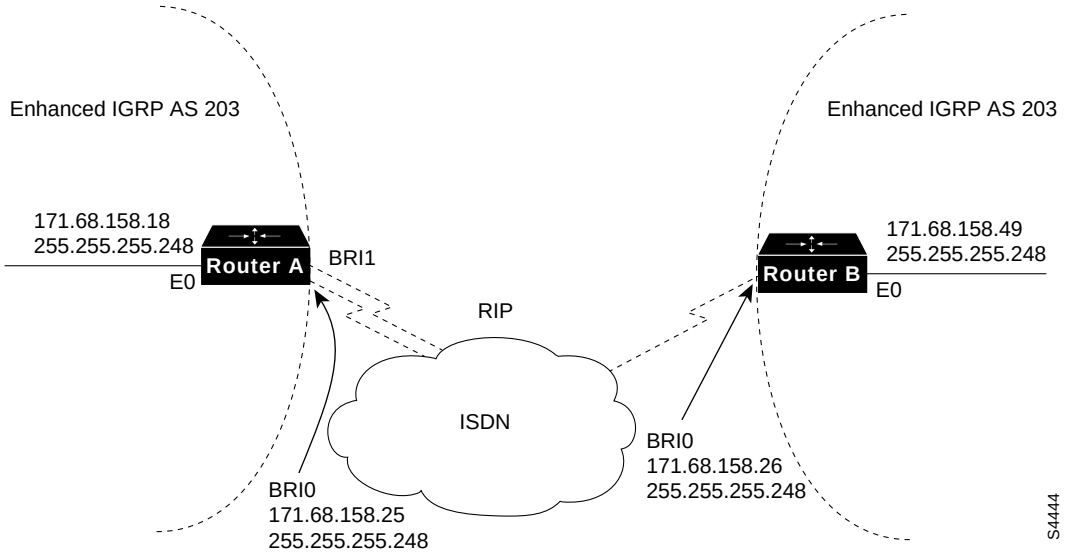
For a snapshot routing configuration example, see the chapter “Using ISDN Effectively in Multiprotocol Networks” in the *Internetworking Case Studies* publication.

Using Snapshot Routing with Enhanced IGRP

Because it sends out “hello” packets every 5 seconds to maintain its routing tables, Enhanced IGRP routing protocol updates need to be controlled over ISDN links. Because snapshot routing does not control Enhanced IGRP packets, another technique must be used. One way is to use access lists, as described in the “IP Enhanced IGRP Packets” section later in this chapter.

Another way is to use RIP (which snapshot routing can control) across ISDN links. For the RIP approach to work, RIP information must be redistributed into the Enhanced IGRP networks and vice versa. Figure 11-7 shows a simple network in which IP Enhanced IGRP is used on both LANs with RIP running between the two LANs.

Figure 11-7 Enhanced IGRP-Based Network with RIP for ISDN Links



The following partial configuration shows the commands that configure Router A and Router B for IP Enhanced IGRP, RIP, and route redistribution between the two routing protocols:

```
hostname RouterA
!
router eigrp 203
network 171.68.0.0
redistribute rip
default-metric 128 100 255 1 1500
passive-interface bri 0
!
router rip
network 171.68.0.0
redistribute eigrp 203
default metric 2
distribute-list 1 in
access-list 1 deny ip 171.68.158.48 255.255.255.248
passive-interface ethernet 0

hostname RouterB
!
router eigrp 203
network 171.68.0.0
redistribute rip
default-metric 128 100 255 1 1500
passive-interface bri 0
!
router rip
network 171.68.0.0
redistribute eigrp 203
default metric 2
distribute-list 1 in
access-list 1 deny ip 171.68.158.16 255.255.255.248
passive-interface ethernet 0
```

To prevent routes that are redistributed into Enhanced IGRP from RIP from being redistributed back into RIP and creating a routing loop, the configurations include the **distribute-list in** router configuration command for RIP and Enhanced IGRP to control which routes are passed back and

forth. The **distribute-list in** command causes the router to use access list 1 to filter networks learned from RIP and allows only those networks that match the list to be redistributed into Enhanced IGRP. This prevents route feedback loops from occurring.

The **default-metric** router configuration command in the Enhanced IGRP portion of the configuration assigns an Enhanced IGRP metric to all RIP-derived routes. The first value (128) specifies a minimum bandwidth of 128 kbps. The second value (100) specifies a route delay in tens of microseconds. The third value (255) specifies the connection is guaranteed to be 100 percent reliable. The fourth value (1) specifies the effective bandwidth of the route. The fifth value (1500) specifies in bytes the maximum transmission unit (MTU) of the route.

The **default-metric** router configuration command in the RIP portion of the configurations causes RIP to use the same metric value (in this case, a hop count of 2) for all routes obtained from Enhanced IGRP. A default metric helps solve the problem of redistributing routes that have incompatible metrics. Whenever metrics do not convert, using a default metric provides a reasonable substitute and enables the redistribution to proceed.

The **passive-interface** router configuration command declares an interface to be passive. When an interface is passive, Enhanced IGRP excludes the interface from routing update broadcasts. If you do not want to run RIP across the ISDN link, you can use the **passive-interface** command and static routes.

Access Lists

Depending on the protocols that your network runs, you might need to use access lists to control routing update packets that snapshot routing does not control. Or, depending on your network design, you might not be able to use snapshot routing, in which case, access lists must be used to control routing updates. This section describes access list techniques for controlling the following types of traffic:

- IP Enhanced IGRP Packets
- SNMP Packets
- Banyan VINES, DECnet IV, and OSI Packets
- IPX Packets

IP Enhanced IGRP Packets

You can use one of the following two access lists to control Enhanced IGRP traffic:

```
access-list 101 deny eigrp any any
access-list 101 deny ip any 224.0.0.10 0.0.0.0
```

The first access list denies all Enhanced IGRP traffic and the second access list denies the multicast address (224.0.0.10) that Enhanced IGRP uses for its updates. When you use access lists to control Enhanced IGRP traffic, you need to configure static routes to create routes across the ISDN link.

SNMP Packets

Although SNMP can provide useful information about ISDN connections and how they are used, using SNMP can result in excessive up time for ISDN links. For example, HP OpenView gathers information by regularly polling the network for SNMP events. These polls can cause the ISDN connections to be made frequently in order to check that the remote routers are there, which results in higher ISDN usage charges. To control ISDN charges, the central site should filter SNMP packets destined for remote sites over ISDN. Incoming SNMP packets from remote sites can still be permitted, which allows SNMP traps to flow to the SNMP management platform. That way, if an SNMP device fails at the remote site, the alarm will reach the SNMP management platform at the central site.

To control SNMP traffic, create an access list that denies SNMP packets. The following is an example of SNMP filtering:

```
access-list 101 deny tcp any any eq 161
access-list 101 deny udp any any eq snmp
access-list 101 permit ip any any
!
dialer-list 1 list 101
```

Note The preceding example uses two **access-list** commands because the Layer 3 SNMP protocol can be either TCP or UDP. If your network uses IPX SNMP, you must create a separate access list.

Banyan VINES, DECnet IV, and OSI Packets

Cisco IOS Software Release 10.3 introduces access lists for Banyan VINES, DECnet IV, and the Open Systems Integration (OSI) protocol. When a dialer map is configured for these protocols, access lists can be used to define *interesting* packets (that is, packets that will trigger the DDR link).

IPX Packets

You can use access lists to declare as *uninteresting* packets intended for the Novell serialization socket (protocol number 0, socket number 457), RIP packets (protocol number 1, socket number 453), SAP packets (protocol number 4, socket number 452), and diagnostic packets generated by the autodiscovery feature (protocol number 4, socket number 456). Uninteresting packets are dropped and do not cause connections to be initiated. For a sample IPX access list, see the chapter “Using ISDN Effectively in Multiprotocol Networks” in the *Internetworking Case Studies* publication.

Protocol-Specific Techniques

This section describes techniques that supplement snapshot routing and access lists for the following protocols:

- IPX
- AppleTalk

IPX

IPX sends out several types of packets that, if not controlled, cause unnecessary connections: IPX watchdog packets and SPX keepalive packets. In addition, NetWare includes a time synchronization protocol that, if not controlled, causes unnecessary connections.

Controlling IPX Watchdog Packets

NetWare servers send "watchdog" packets to clients and disconnect any clients that do not respond. When IPX watchdog spoofing is enabled, the router local to the NetWare server responds to watchdog packets on behalf of the server's clients. IPX watchdog spoofing allows clients to remain attached to servers without having to constantly send packets across the ISDN link to do so. This feature is particularly important when trying to control ISDN link up time. The interface configuration command for enabling IPX watchdog spoofing is **ipx watchdog-spoof**.

Controlling SPX Keepalive Packets

Some Sequenced Packet Exchange (SPX)-based services in the Novell environment use SPX keepalive packets. These packets are used to verify the integrity of end-to-end communications when guaranteed and sequenced packet transmission is required. The keepalive packets are generated at a rate that can be adjusted by the user from a default of one every 5 seconds to a minimum of one every 15 minutes. SPX spoofing as implemented in the Cisco IOS software receives, recognizes, and successfully acknowledges keepalive packets both at the server end and the client end.

Time Server and NDS Replica Packets

NetWare 4.*x* includes a time synchronization protocol that causes NetWare 4.*x* time servers to send an update every 10 minutes. To prevent the time server from generating update packets that would cause unwanted connections, you need to load a NetWare-loadable module (NLM) named TIMESYNC.NLM that allows you to increase the update interval for these packets to several days.

A similar problem is caused by efforts to synchronize NDS replicas. NetWare 4.1 includes two NLMs, DSFILTER.NLM and PINGFILT.NLM, that work together to control NDS synchronization updates. Use these two modules to ensure that NDS synchronization traffic is sent to specified servers only at the specified times.

AppleTalk

The AppleTalk Name Binding Protocol (NBP) converts entity names into numeric addresses. NBP can transmit a significant amount of traffic throughout the network regardless of the named entity's location. This in turn can cause excessive dial-on-demand triggers. Applications such as QuarkXpress and 4D use all zone NBP broadcasts to periodically probe the network either for licensing purposes or to provide links to other networked resources. The **debug apple nbp** command with the **debug dialer** command monitors NBP traffic and can help you determine the kinds of packets that cause connections to be made.

NBPTEST, an option when executing an AppleTalk **ping** command, is also useful when locating particular nodes that are transmitting NBP broadcasts.

Beginning with Cisco IOS Software Release 11.0, you can filter NBP packets based on the name, type, and zone of the entity that originated the packet. AppleTalk NBP filtering allows Cisco routers to build firewalls, dial-on-demand triggers, and queuing options based on any NBP type or object. For a configuration example, see "Using ISDN Effectively in Multiprotocol Networks" in the *Internetworking Case Studies* publication.

Ultimately, if the applications that use NBP have been isolated, consult the individual vendors and ask for their advice on how to control or eliminate NBP traffic.

Performance

This section describes the following techniques for using multiple B channels:

- Bandwidth on Demand
- PPP Multilink
- Dialer Rotary Groups

This section also describes the following techniques for using ISDN bandwidth effectively:

- Compression
- Dial Backup for Leased Lines

Bandwidth on Demand

Bandwidth on demand allows you to use the second B channel of a BRI. When used with a BRI, bandwidth on demand doubles the bandwidth across the link—from 56/64 kbps to 112/128 kbps.

To configure an interface to use bandwidth on demand, use the **dialer load-threshold** interface configuration command, which specifies a load (a value between 1 and 255) beyond which another call to the destination is to be initiated. When applied to BRIs, the **dialer load-threshold** command brings up the second B channel. In the following partial configuration example, the second B channel is activated when the first B channel is at 50 percent usage.

```
interface bri 0
ip address 171.68.158.26 255.255.255.248
encapsulation ppp
dialer map ip 171.68.158.25 name RouterA speed 64 14085551111
dialer load-threshold 128
dialer-group 1
ppp authentication chap
```

Note Bandwidth on demand is a protocol-independent technique and is not specific to ISDN. The **dialer load-threshold** command can only be used with dialer rotary groups. By default, each ISDN interface is a dialer rotary group.

PPP Multilink

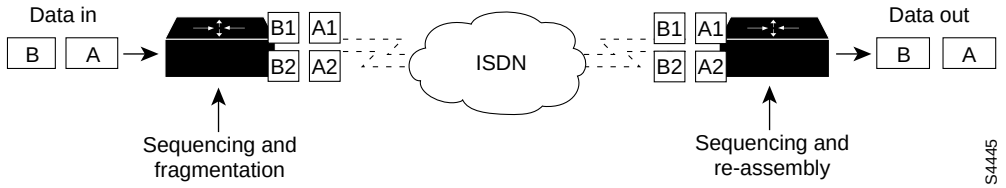
PPP Multilink (MP) is an Internet Engineering Task Force (IETF) standard (RFC 1717) for aggregating B channels that allows for multivendor interoperability. MP defines a way of sequencing and transmitting packets over multiple physical interfaces. To reduce potential latency issues, MP also defines a method of fragmenting and reassembling large packets that can be used for protocols that do not tolerate out-of-order packets, such as AppleTalk and IPX.

It is important to note that MP does not define how or why connections should be initiated or torn down. The design of this mechanism has been left to the vendors. Cisco's implementation allows the user to define a load factor (the percentage of bandwidth being used on a B channel) at which point a second or subsequent B-channel call should be initiated. The load factor can be defined for incoming data only, outgoing data only, or for both. This allows MP to be used effectively in many different environments, such as collecting information from the World Wide Web (mostly incoming traffic) and sending files to colleagues (mostly outgoing traffic).

Figure 11-8 illustrates a basic MP session in which MP has already brought a second B channel into operation. Incoming packets A and B are both fragmented into smaller packets, given a sequence number (A1, A2, B1, and B2), and shared over the two B channels. (All packets greater than 30 bytes

in length are subject to fragmentation.) When the fragments of packets A and B arrive at the receiving router, MP reassembles the original packets and sequences them correctly in the data stream.

Figure 11-8 PPP Multilink



Note MP is currently processed switched. You need to consider performance in large hub implementations that have multiple ISDN PRIs.

With constantly changing MP software on different vendors' ISDN products, PPP interoperability can never be guaranteed. To reduce interoperability problems, Cisco regularly participates in PPP interoperability testing. For the latest test results, consult your technical support representative.

MP can be used with any Cisco ISDN BRI or PRI interface. MP can be used with other ISDN features, such as PPP authentication, PPP compression (described in the "Compression" section later in this chapter), PPP callback (described in the "Callback" section later in this chapter) and IP address negotiation (described in the "IP Address Negotiation for ISDN" section earlier in this chapter).

Dialer Rotary Groups

To increase the bandwidth of an ISDN connection beyond the 128-kbps limit of a single BRI, aggregate multiple BRIs.

Step 1 Use the **dialer rotary-group** command to assign each BRI to a dialer rotary group.

Step 2 Use the **interface dialer** command to create a dialer interface.

Step 3 Apply network addresses and **dialer map** commands to the dialer interface.

Step 4 Use the **dialer load-threshold** command to bring into operation multiple ISDN BRIs in the rotary group based on traffic thresholds.

The following partial configuration for Router A aggregates its two BRIs:

```
interface bri 0
dialer rotary-group 1
interface bri 1
dialer rotary-group 1
interface dialer 1
dialer load threshold 128
ip address 171.68.158.26 255.255.255.248
dialer map ip 171.68.158.27 name RouterC speed 64 4085551212
```

Compression

The Point-to-Point (PPP) Compression Control Protocol (CCP) is an Internet Engineering Task Force (IETF) draft RFC that defines a method for negotiating data compression over PPP links. These links can be either leased lines or circuit-switched WAN links, including ISDN. Compression increases throughput and shortens file transfer times.

Use the **compress** interface configuration command at both ends of the link to enable compression. Use the **stac** keyword to enable the Stacker (LZS) compression algorithm or the **predictor** keyword to enable the RAND algorithm (a predictor algorithm). The Stacker algorithm is appropriate for LAPB and PPP encapsulation, and the RAND algorithm is appropriate for HDLC and PPP encapsulation. The Stacker algorithm is preferred for PPP encapsulation.

Dial Backup for Leased Lines

Dial backup protects against wide-area network (WAN) downtime by allowing a dedicated serial connection to be backed up by a circuit-switched connection. To configure dial backup, associate an interface (in this case, an ISDN interface) as a backup to a primary serial interface.

Once configured, the dial backup interface remains inactive until one of the following conditions is met:

- The primary line goes down—When the Carrier Detect signal from the primary line device is lost or when the line protocol goes down, the backup line is activated, preserving the connection between the two sites.
- The transmitted traffic load on the primary line exceeds a defined limit—The traffic load is monitored and a 5-minute moving average is computed. If the average exceeds the user-defined value for the line, the backup line is activated. Depending on how the backup line is configured, some or all of the traffic flows onto it.

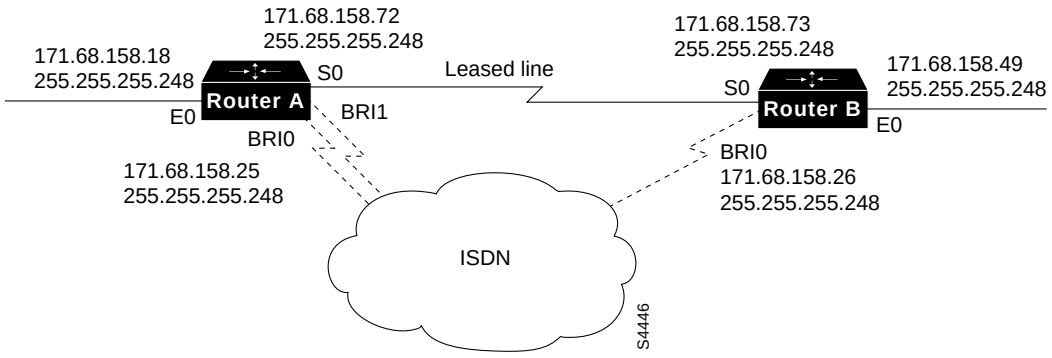
The following interface configuration commands, applied to the primary interface, establish a dial backup:

- The **backup interface** interface configuration command specifies the interface that is to act as the backup.
- The **backup load** command specifies the traffic threshold at which the backup interface is to be activated and deactivated.
- The **backup delay** command specifies the amount of time that is to elapse before the backup interface is activated or deactivated after a transition on the primary interface.

Note An interface can be configured as the backup for one interface only—it cannot be configured as the backup for multiple interfaces.

In Figure 11-9, a leased line connects Router A to Router B, and BRI 0 on Router B is used as a backup line.

Figure 11-9 Example of Dial Backup over ISDN



Note For simplicity, this example shows IP addressing. Other protocols can also be configured.

In the following partial configuration example for Router B, BRI 0 is activated only when serial interface 0 (the primary line) goes down. The **backup delay** command configures the backup connection to activate 30 seconds after serial interface 0 goes down and to remain activated for 60 seconds after the serial interface 0 comes up.

```
interface serial 0
ip address 171.68.158.73
backup interface bri 0
backup delay 30 60
```

In the following partial configuration example for Router B, BRI 0 is activated only when the load on serial 0 (the primary line) exceeds 75 percent of its bandwidth. The backup line is deactivated when the aggregate load between the primary and backup lines is within 5 percent of the primary line's bandwidth.

```
interface serial 0
ip address 171.68.158.73
backup interface bri 0
backup load 75 5
!
```

In the following partial configuration example for Router B, BRI 0 is activated only when serial interface 0 goes down or when traffic on serial interface 0 reaches exceeds 25 percent. If serial interface 0 goes down, 10 seconds will elapse before BRI 0 becomes active. When serial interface 0 comes up, BRI 0 will remain active for 60 seconds. If BRI 0 is activated because the traffic on serial interface 0 exceeds 25 percent, BRI 0 is deactivated when the aggregate load of serial interface 0 and BRI 0 returns to within 5 percent of the bandwidth of serial interface 0.

```
interface serial 0
ip address 171.68.158.73
backup interface bri 0
backup load 25 5
backup delay 10 60
```

Security

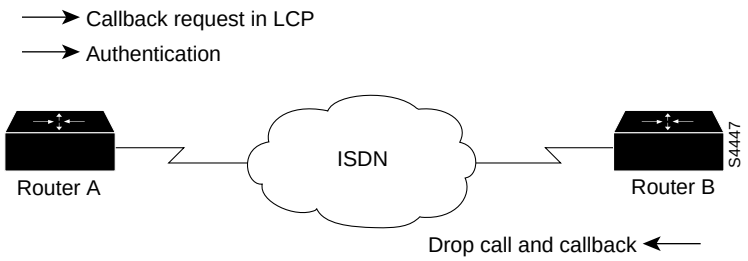
ISDN includes several features that you can use to increase the security of ISDN connections:

- Callback
- Screening
- Called Party Number Verification
- Calling Number Identification

Callback

Callback allows a router (typically a remote router) to initiate a circuit-switched WAN link to another device and request that device to call back. The device, such as a central site router, responds to the callback request by calling the device that made the initial call. Callback uses the Point-to-Point Protocol (PPP) and the facilities specified in RFC 1570. Figure 11-10 shows a typical negotiation.

Figure 11-10 ISDN Callback



In Figure 11-10, callback is completed in the following sequence of steps:

Step 1 Router A brings up a circuit-switched connection to Router B.

Step 2 Routers A and B negotiate PPP Link Control Protocol (LCP). Router A can request a callback, or Router B can initiate a callback.

Step 3 Router A authenticates itself to Router B using PPP PAP or CHAP. Router B can optionally authenticate itself to Router A.

Step 4 Both routers drop the circuit-switched connection.

Step 5 Router B brings up a circuit-switched connection to Router A.

Callback provides centralized billing for synchronous dial-up services. It also allows you to take advantage of tariff disparities on both a national and international basis. However, because callback requires a circuit-switched connection to be established before the callback request can be passed, a small charge (dependent on local tariffing) is always incurred by the router initiating the call that requests a callback. See “Using ISDN Effectively in Multiprotocol Networks” in the *Internetworking Case Studies* publication for a callback configuration example.

Screening

Some central office switches support caller ID, which allows the router to verify that an incoming call comes from an expected source. If you configure caller ID screening but your central office switch does not support it, the router will reject all calls.

The **isdn caller** interface configuration command configures caller ID screening. For example, the following command configures a BRI to accept a call with a delivered caller ID having 41555512 and any numbers in the last two positions:

```
isdn caller 41555512xx
```

Called Party Number Verification

When multiple devices and a router share the same ISDN local loop, you can ensure that the correct device answers an incoming call by configuring the device to verify the called party number and the subaddress delivered by the switch as part of the setup message against the device's configured number and subaddress.

To configure called party number verification on the router, apply the **isdn answer1** or **isdn answer2** interface configuration command to the BRI. These commands allow you to specify the called party number or the subaddress number, or both.

If you do not use the **isdn answer1** command or the **isdn answer2** command, the router processes and accepts all incoming calls.

Calling Number Identification

This feature applies only to routers used in Australia. A router that connects to a Australian TS013 or TS014 central office switch may want to supply the network with a billing number for outgoing calls. The Australian network offers a better tariffing on calls in which the number is presented.

To configure the interface to identify the billing number, use the **isdn calling number** interface configuration command.

Network Management

The Simple Network Management Protocol (SNMP) uses management information bases (MIBs) to store information about network events. Currently, no industry-standard ISDN MIB is available, but as of Cisco IOS Software Release 10.3(3), two Cisco ISDN MIBs are available. With these MIBs, SNMP-compliant management platforms (for example, HP OpenView or SunNet Manager) can query Cisco routers for ISDN-related statistics.

The Cisco ISDN MIB focuses primarily on ISDN interface and neighbor information. It defines two MIB groups: *demandNbrTable* and *demandNbrEntry.* Table 11-5 lists some of the MIB variables that are available in the ISDN MIB.

Table 11-5 Cisco ISDN MIB Variables

MIB Object	Description
demandNbrPhysIf	Index value of the physical interface that the neighbor will be called on; on an ISDN interface, this is the ifIndex value of the D channel
demandNbrMaxduration	Maximum call duration in seconds
demandNbrLastduration	Duration of last call in seconds
demandNbrAcceptCalls	Number of calls accepted from the neighbor
demandNbrRefuseCalls	Number of calls from neighbor that the router has refused

The Cisco Call History MIB stores call information for accounting purposes. The goal is to provide a historical view of an ISDN interface, including the number of calls that have been placed and call length. Most call history MIB variables are in the *ciscoCallHistory* MIB group. Table 11-6 lists some of the MIB variables.

Table 11-6 Cisco Call History Variables

MIB Object	Description
ciscoCallHistoryStartTime	The value of sysUpTime when this call history entry was created; this variable can be used to retrieve all calls after a specific time
ciscoCallHistoryCalledNumber	The number that was used to place this call
ciscoCallHistoryCallConnectionTime	The value of sysUpTime when the call was connected
ciscoCallHistoryCallDisconnectTime	The value of sysUpTime when the call was disconnected

The Cisco ISDN MIBs assume SNMP support on the network. If an SNMP-compliant management platform is present, the Cisco ISDN MIBs deliver valuable information about ISDN links. In particular, the Call History MIB provides critical information about ISDN up time, which is useful for tracking ISDN charges.

Summary

Cisco offers a wide range of ISDN-based products in response to a variety of internetworking needs. The Cisco IOS software provides a number of features that maximize ISDN performance and minimize ISDN usage charges, such as snapshot routing, access lists, NBP filtering (for AppleTalk), and watchdog and keepalive packet control (for IPX).