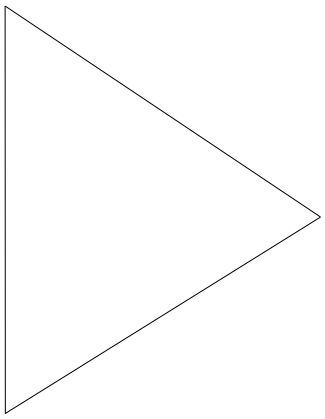
Design Implementation Guide



August 1995

Integrated Services Digital Network (ISDN) Services

Authored by Jeffrey Baher, **Technical Marketing**
(jbaher@cisco.com)

Overview

Basic rate and primary rate Integrated Services Digital Network (ISDN) services are rapidly establishing footholds in the networking and communications arenas. And as this happens, more and more network environments are turning to ISDN to solve a variety of wide-area networking connectivity problems. In particular, ISDN is rapidly gaining acceptance for telecommuting applications.

Cisco Systems recognizes both the tremendous potential that ISDN offers as well as the growing need to provide effective ISDN-based solutions. In doing so, Cisco acknowledges that ISDN presents a new paradigm in networking, and as such, needs to be addressed differently than other technologies. The ISDN networking paradigm is based on addressing and managing two critical issues:

- Bandwidth conservation
- Tariff/link management

Through advanced features in the Cisco Internetwork Operating System (Cisco IOS™) software, Cisco addresses both of these issues. With features such as snapshot routing, IPX/SPX spoofing, and data compression, Cisco has been able to deliver an effective ISDN internetworking solution to all of its ISDN-based product offerings.

The document that follows serves as a foundation for ISDN internetworking with Cisco. It begins with a brief overview of Cisco's ISDN-based product line and some of the key ISDN-related Cisco IOS features. Next is a detailed discussion of the various ISDN design scenarios, followed then by a detailed discussion on how to configure various features to enable ISDN connectivity. In the end, the goal is to provide a solid understanding of ISDN and how to best develop effective and efficient internetworking solutions with Cisco hardware and software products.

ISDN Overview

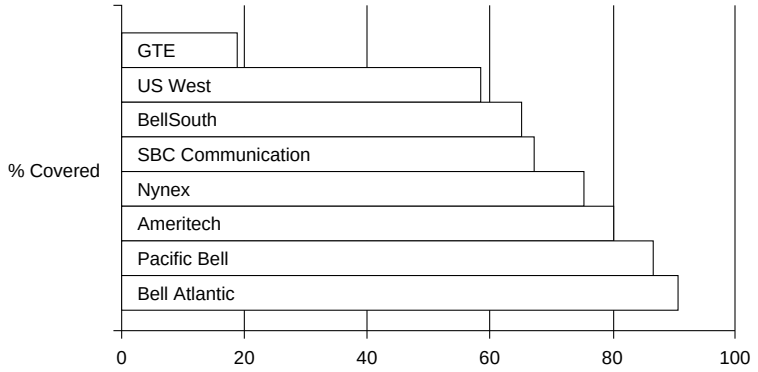
Integrated Services Digital Network (ISDN) refers to a set of digital services that are rapidly becoming available to end users. ISDN involves the digitization of the telephone network so that voice, data, text, graphics, music, video, and other source material can be provided to end users from a single terminal over existing telephone wiring. Visions of the future show ISDN deployed in a worldwide network much like the present telephone network, except that digital transmission serves as the foundation for a gamut of services.

Besides voice and the other applications listed above, ISDN looks to deliver additional capabilities including high-speed image applications (such as Group IV facsimile), additional data lines in homes to serve the telecommuting industry, high-speed file transfer, and videoconferencing.

CISCO SYSTEMS

Many carriers are beginning to offer ISDN under tariff. In North America, large local-exchange carriers (LECs) are beginning to provide ISDN service as an alternative to the T1 connections (digital carrier facilities provided by telephone companies) that currently carry bulk wide-area telephone service (WATS) services. Figure 1 shows leading U.S. telecommunications companies and their projected ISDN penetrations by the end of 1995.

Figure 1. ISDN Coverage of U.S. Telecommunications Companies



As the ISDN technology grows, so too do Cisco Systems' product offerings. Currently Cisco offers both Basic Rate Interface (BRI) and Primary Rate Interface (PRI) ISDN products. Each BRI interface delivers two 64-kbps data channels (B channels) and one 16-kbps signaling channel (D channel). The BRI service is commonly referred to as 2B+D. The PRI interface delivers twenty-three 64-kbps B channels and one 64-kbps D channel for T1 links (23B+D) and thirty 64-kbps B channels and one 64-kbps D channel for E1 links (30B+D). For a discussion of ISDN technology, refer to Appendix A.

The AccessPro PC Card, Cisco 1003, Cisco 2503, Cisco 2504, Cisco 2516, and Cisco 2517 products deliver single-port ISDN BRI service, while the Cisco 4000 series with one MBRI network processor module (NPM) delivers either four or eight BRI ports. For PRI, both the Cisco 4000 series and Cisco 7000 series routers offer Primary Rate services. In addition, the Cisco Internetworking Operating System (Cisco IOS™) software, which runs on the above platforms to deliver routing and bridging functionality, incorporates critical features for effectively deploying and managing ISDN with Cisco routers.

Table 1 lists Cisco's current ISDN-based product offerings and describes the scope of their ISDN support.

Table 1. Cisco ISDN-Based Products

Product	ISDN Support
AccessPro PC Card	1 ISDN BRI interface
Cisco 1003	1 ISDN BRI interface
Cisco 2503/4	1 ISDN BRI interface
Cisco 2516/17	1 ISDN BRI interface
Cisco 4000 Series (per NPM)	4 or 8 BRI interfaces
Cisco 4000 Series (per NPM)	1 PRI interface
Cisco 7000 Series (per MIP[1] controller)	1 or 2 PRI interfaces

1. MIP = Multichannel Interface Processor

The Cisco IOS software includes the following features for ISDN links:

- Dial-on-Demand Routing
- Bandwidth on Demand

- IPX Spoofing
- Snapshot Routing
- PPP CHAP/PAP Authentication
- ISDN MIB

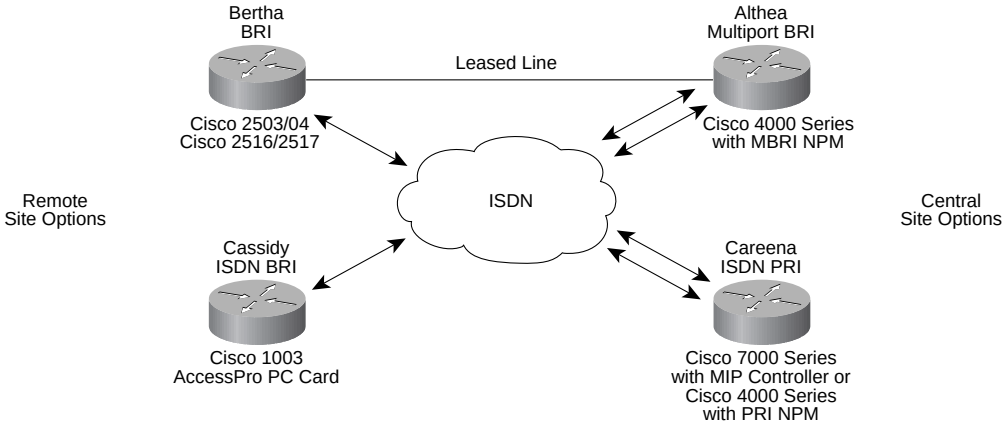
Designing Cisco-Based ISDN Networks

With the current Cisco product offerings in conjunction with the Cisco IOS dial-on-demand routing (DDR) features, there are a variety of different network design options that take advantage of both ISDN BRI and PRI services. In this section, four network designs will be discussed:

- Remote site BRI to central site PRI
- Remote site BRI to central site multiple BRI
- Small office/home office BRI to central site BRI or PRI
- BRI dial backup for leased-line facilities

Figure 2 shows a network topology that integrates these four scenarios.

Figure 2. ISDN-Based Network Design Scenarios



Remote Site BRI to Central Site PRI

In this design, remote site Ethernet or Token-Ring LANs (Cassidy and/or Bertha) access central site resources (Careena) via BRI to PRI sessions. Each remote site router is equipped with BRI service that yields two 64-kbps B channels for data and one 16-kbps D channel for ISDN signaling information. One or both of the B channels can be used to connect back to the central site router. At the central site, incoming calls terminate at a Cisco 7000 series router equipped with a T1 or E1 MIP controller. Each MIP controller interface (one or two interfaces per MIP card) can support one ISDN PRI service. With the T1 MIP controller this yields 23 B channels and one 64-kbps D channel per MIP controller interface. With the E1 MIP controller, this yields 30 B channels and one 1 64-kbps D channel.

Remote Site BRI to Central Site Multiport BRI

In this configuration, remote site Ethernet or Token Ring LANs (Bertha) access central site resources via BRI sessions (Althea). Each remote site router is equipped with BRI service that yields two 6-kbps B channels for data and one 16-kbps D channel for ISDN signaling information. One or both of the B channels can be used to connect back to the central site router. Alternatively, one B channel can connect to one site while the other B channel connects to another site. At the central site, incoming calls terminate at a Cisco 4000 series router equipped with the MBRI NPM. The MBRI NPM delivers either four or eight BRI connections for branch office or telecommuting connectivity. If desired, two MBRI NPMs can be used in a Cisco 4000 series router to get up to 16 BRI interfaces.

Small Office/Home Office BRI to Central Site BRI or PRI

This design is similar to the preceding two designs, although the focus in this case is on simple connectivity (Cassidy to Careena or Althea). The Cisco 1003 is a small, inexpensive unit with one Ethernet port and one ISDN port. There is no Token Ring option. The Cisco 1003 supports IP, IPX, and AppleTalk routing, and bridging for other protocols. Cisco's AccessPro PC card is also ideal for small offices or home offices. The AccessPro PC card is an ISA card that installs in a PC chassis and runs all of the Cisco IOS software. The AccessPro, however, does not rely on the PC for route processing. All routing functionality resides on the card itself. The AccessPro PC Card is available in a variety of configurations, including one with either one Ethernet or one Token Ring port and one ISDN port.

BRI Dial Backup for Leased-Line Facilities

In this design, ISDN is used as a backup for a leased-line connection between Bertha and Althea. If the primary link (T1 or fractional T1) goes down, an ISDN circuit-switched connection is established and traffic is rerouted over ISDN. When the primary link is restored, traffic will be rerouted to the leased line, and the ISDN link will be 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 will be brought up to increase bandwidth between the two sites.

ISDN Implementation: ISDN Basic Configuration

As with any network design, it is important to do some up-front thinking before beginning the actual network installation. In particular, take the time to plan out network addressing, routing designs, and security. Additionally, when dealing with ISDN it is also important to consider cost structures. Typically, ISDN is tariffed based on uptime. Simply put, when the link is up, charges are incurred. The goal should be to keep uptime to a minimum without sacrificing end-user connectivity.

Configuration Steps

There are two principal sets of commands needed to bring up an ISDN link between two LANs. The first set are ISDN-related commands, while the second set are Point-to-Point Protocol (PPP) related. Some of these commands are global configuration commands and others are interface configuration commands.

ISDN-Specific Commands

The following are ISDN-specific commands necessary for bringing up an ISDN link. (For PRI configuration information refer to the section entitled "ISDN Implementation: Advanced Topics" later in this document.)

- **isdn switch-type** <*switch type*>

  The Cisco IOS software supports a variety of ISDN switch types. To examine the supported switches, type **isdn switch-type ?** . An ISDN switch type must be specified. The switch type refers to the switch that the Central Office (CO) is using. Consult your carrier to find out which switch it is using. Note that in some cases, the switch type will be country specific.

- **isdn tei [first-call]** or **[powerup]**

  This command determines when Layer 2 ISDN Terminal Endpoint Identifier (TEI) negotiation occurs. The default is set for negotiation to occur when the router is powered on. TEI negotiation is useful in Europe and for switches that might deactivate layer 2 when no calls are active. *In most cases, this command can be omitted.*

- **isdn spid1** <*spid number*> <**[ldn (optional)]**>

  Depending on the ISDN switch and the software version that the switch is running, this command may or not be required. SPIDs are only used in North America. If the switch is a DMS-100 or a National ISDN-1 (NI-1) switch, Service Profile Identifiers (SPIDs) are required. The AT&T 5ess switch may also require SPIDs depending on the version of software that the 5ess is running. Consult your service provider to determine if SPIDs are needed.

  A SPID is a number provided by the ISDN carrier to identify the line configuration of the BRI service. Each SPID points to line setup and configuration information. When a device is plugged in to the ISDN network, it performs a D-channel layer 2 initialization process whereby a TEI is assigned to the device. The device then attempts D-channel layer 3 initialization. If a SPID is necessary but not configured on the device, the device fails the D-channel layer 3 initialization and calls cannot be placed.

  An AT&T 5ess can support up to eight SPIDs per BRI line. Because multiple SPIDs can be applied to a single B channel, multiple services can be supported simultaneously. For example, the first B channel can configured for data, and the second B channel can be configured for both voice and data. In this scenario, the second B channel can support an ISDN telephone in addition to supporting data connections. For 5ess switches, the SPID is the 10-digit ISDN number prepended by “01” and appended by “0.”

```
Example:    ISDN number: 4085551212
            SPID: 0140855512120
```

  DMS-100 and NI-1 switches only support two SPIDs with only one B channel per SPID. If both B channels will be used for data only, enter the two SPIDs (one for each B channel). An issue comes up when trying to run data and voice over the same B channel. Assuming the first SPID is applied to the first B channel for data traffic and is limited to that B channel only, this leaves only one other SPID for the second B channel. Consequently, the second B channel can be used for either data or voice but not both simultaneously. The absence or presence of the second SPID in the router’s configuration dictates whether the second B channel can be used for data or voice. Below is an example of SPID values for DMS-100 and NI-1 switches. In this case the SPID is the 10-digit ISDN number appended by a “01” for SPID 1 and a “02” for SPID 2.

```
Example:      ISDN number: 4085551212
              SPID 1: 408555121201
              SPID 2: 408555121202
```

  Note: There is no standard format for SPIDs. As a result, SPID values can vary depending on the switch vendor and the carrier. The examples above are intended only as examples.

  The LDN, or local directory number, is delivered by the service provider in the incoming setup message. The LDN value is optional and is not necessary for establishing ISDN-based connections. This is a seven-digit number assigned by the service provider. You must define the LDN if you want to receive any incoming calls on the B2 channel. The ISDN switch checks for the LDN to determine whether both channels can be used to transmit and receive data. If the LDN is not present, then only the B1 channel can be used for full-duplex communication. However, the other channel can still be used to make outgoing calls.

  ISDN debugging tools can help determine if SPIDs are needed or misconfigured. Refer to the “ISDN Debugging” section that follows for more information.

- **isdn spid2** <*spid number*> **[ldn]**

  Use this command to enter a second SPID number.

PPP-Specific Commands

The following are PPP-specific commands necessary for bringing up an ISDN link:

- ppp encapsulation

This command sets PPP encapsulation for a given interface. The BRI interface supports High-Level Data Link Control (HDLC), PPP, X.25, and Frame Relay encapsulations. Unless there is a need for a particular encapsulation, PPP encapsulation is recommended, with Challenge Handshake Authentication Protocol (CHAP) authentication for added security.

- **username** <*name*> **password** <*password*>

  This command is used for PPP CHAP and Password Authentication Protocol (PAP) authentication. Add a username entry for each remote router that the local router communicates with and for which it requires authentication. If both sides of the ISDN link are running PPP and PAP, a username entry and password must also be present for the local router.

  Note: Usernames are case sensitive.

- ppp authentication chap/pap

  This command enables either CHAP or PAP authentication.

  While either CHAP or PAP authentication can be used, CHAP does offer added security. PAP sends clear text passwords over the link, and it provides no protection from playback. CHAP, on the other hand, sends only encrypted information across the link and never sends the actual passwords.

  Note: The password used for each pair of routers that communicate using PAP or CHAP must be the same. See the following example.

Configuration	Router yyy	Router xxx	Router zzz
hostname	yyy	xxx	zzz
interface serial	0	0	0
encapsulation	ppp	ppp	ppp
ppp authentication	chap	chap	chap
user name xxx password	secretxy	secretxy	secretxz
user name zzz password	secretzy	secretxz	secretzy

ISDN Debugging

The Cisco IOS software includes extensive debugging tools. From either the console port or via a Telnet (VTY) session, users can access debugging information. Below are the basic commands for enabling and disabling Cisco IOS debugging. These commands are top-level commands and cannot be accessed if the router is in global or interface configuration mode. Note that multiple debugging operations can run simultaneously.

- **debug** <*debug topic*>

  Use this command to enable debugging. To browse the available debugging options, type **debug ?** .

- **undebug** <*debug topic*> or **all**

  This command turns debugging off. If multiple debug operations are running, typing **undebug all** provides an easy way to disable all debugging. Individual debugging operations can be disabled as well.

- terminal monitor

  This command is necessary for Telnet (VTY) sessions. This command enables the display of debugging information. Without this command, debugging information will only be displayed on console connections. Each Telnet (VTY) session will have to enter this command.

The Cisco IOS software includes three ISDN-specific debugging tools:

- debug isdn-event
- debug isdn q.921
- debug isdn q.931

ISDN-event

Use the **debug isdn-event** command to display events occurring on the user side of the ISDN interface. The ISDN events may be Q.931 events (call setup and teardown of ISDN circuits).

The following is a sample output when **debug isdn-event** is enabled; it shows output of call setup events for an incoming call:

```
received HOST_INCOMING_CALL
      Bearer Capability i = 0x080010
      ---------------------------------
      Channel ID i = 0x0101
      Calling Party Number i = 0x0000, `415555121202'
      IE out of order or end of `private' IEs --
      Bearer Capability i = 0x8890
      Channel ID i = 0x89
      Calling Party Number i = 0x0083, `415555121202'
received HOST_INCOMING_CALL
ISDN Event: Received a call from 415555121202 on B1 at 64 Kb/s
ISDN Event: Accepting the call
received HOST_CONNECT
    Channel ID i = 0x0101
ISDN Event: Connected to 415555121202 on B1 at 64 Kb/s
```

The **debug isdn-event** command can also be useful for determining whether or not a SPID is needed or if a SPID is misconfigured.

The following is sample output from **debug isdn-event** showing misconfigured SPID messages:[1]

```
11678.060 TX -> INFORMATION pd=8 callref=(null)
     SPID Information i=0x31323334353536373736
11678.164 RX <- INFORMATION pd=8 callref=(null)
     Cause i = 0x82E43- Invalid IE contents
ISDN Event: incoming ces value=1
received HOST_TERM_REGISTER_NACK - invalid EID/SPID
     or TEI not assigned
     Cause i = 0x8082- No route to specified network
```

ISDN Q.921

Debug isdn-q921 is intended to display layer 2 procedures. The information displayed is limited to D-channel data link signaling information Link Access Protocol D (LAPD).

The following is sample output for Q.921 debugging; it shows output for a startup message on a DMS-100 switch.[2]

---

1. Refer to the *Debug Command Reference* manual or Cisco Connection Documentation CD-ROM for a detailed description of the debugging output.

```
139.516 TX -> IDREQ ri = 48386 ai = 127
139.520 RX <- IDREM ri = 0 ai = 89
139.544 RX <- IDASSN ri = 48386 ai = 90
139.552 TX -> SABMEp sapi = 0 tei = 90
139.552 RX <- IDCKRQ ri = 0 ai = 127
139.560 TX -> IDCKRP ri = 36131 ai = 90
140.548 RX <- IDCKRQ ri = 0 ai = 127
140.556 TX -> IDCKRP ri = 24404 ai = 90
140.560 TX -> SABMEp sapi = 0 tei = 90
140.548 RX <- Uaf sapi = 0 tei = 90
```

ISDN Q.931

Debug **isdn-q931** displays layer 3 D-channel information including call setup and teardown information between the local router and the network.

The following is sample output for Q.931 debugging; it is part of a call setup procedure for an outgoing call.

```
234191.372 TX -> SETUP pd = 8 callref = 0x04

    Bearer Capability i = 0x8890

    Channel ID i = 0x83

    Called Party Number i = 0x80, '415555121202'

234191.624 RX <- CALL_PROC pd = 8 callref = 0x84

    Channel ID i = 0x89

234191.692 RX <- CONNECT pd = 8 callref = 0x84

234191.692 TX -> CONNECT_ACK pd = 8 callref = 0x04
```

The debug isdn-q931 command can also be helpful for determining whether or not a SPID needs to configured or if a SPID is misconfigured.

The following is sample output from **debug isdn-q931** that shows a misconfigured SPID:[3]

```
11678.060 TX -> INFORMATION pd=8 callref=(null)

    SPID Information i=0x31323334353536373736

11678.164 RX <- INFORMATION pd=8 callref=(null)

    Cause i = 0x82E43- Invalid IE contents
```

Other Debugging Tools

In addition to the ISDN-specific debugging tools, there are some other useful debug commands when working with ISDN.

- **debug dialer—**Displays information about packets traversing DDR links.
- **debug ppp packet—**Displays PPP packets being sent and received. This command displays low-level packet dumps.
- **debug ppp negotiation—**Displays PPP packets transmitted during PPP startup, where PPP options are negotiated.

2. Refer to the *Debug Command Reference* manual or Cisco Connection Documentation CD-ROM for a detailed description of the debugging output.
3. Refer to the *Debug Command Reference* manual or Cisco Connection Documentation CD-ROM for a detailed description of the debugging output.

- **debug ppp error—**Displays protocol errors and error statistics associated with PPP connection negotiation and operation.
- **debug ppp chap—**Displays CHAP packet exchanges and PAP exchanges.

For a detailed description of these and all other debug commands refer to the *Debug Command Reference* manual or Cisco Connection Documentation CD-ROM.

Show Commands

The Cisco IOS software also includes a wide range of "show" commands that display critical information about a router's state. For ISDN and DDR the following "show" commands are useful. To browse the available "show" commands type **show ?** .

Note: Exit out of Configuration mode type (Control Z) before entering "show" commands.

- show controllers bri number

  Check layer 1 of the BRI.

- **show interfaces bri** <*number*> or **show interfaces bri** <*number*> **1 2**

  The first command shows information about the physical attributes of the BRI B and D channels. The second command provides similar information although it breaks out the two B channels.

- **show interfaces serial** <*slot/port*> <*B-channel number*>

  Shows information about the physical attributes of the PRI over T1 B and D channels. The B-channel number takes a value between 1 and 23. This command can be used for E1 PRI as well. In this case, the B-channel number takes a value between 1 and 31.

- **show isdn [memory] [timers] [status] [service]**

  Shows information about ISDN memory; layer 2 or 3 timers; layer 1, 2, and 3 D-channel status; or channel service information. The service "show" command is only available on PRI interfaces.

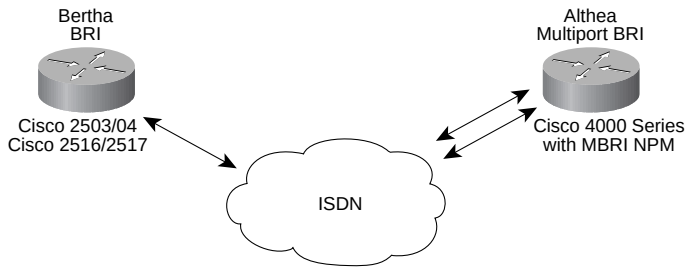
- show dialer

  Shows DDR status on each DDR interface.

ISDN Configuration Example

The sample configurations shown in Figure 3 are intended to show ISDN-specific configuration information only. These configurations do not include all the necessary information to establish a link between the two sites.

Figure 3. Sample ISDN Configuration



Bertha

```
!
hostname bertha
!
enable password ######
!
username althea password 7 094E5B1739522        :PPP username with encrypted display of password (“7
                                                  094E5B1739522”)
isdn switch-type basic-5ess                     :configures router for specific ISDN switch
interface Ethernet0
ip address 171.68.158.49 255.255.255.248
!
interface BRI0
ip address 171.68.158.26 255.255.255.248
encapsulation PPP                               :specifies PPP encapsulation for the interface
ppp authentication chap                         :specifies PPP CHAP authentication for the interface
!
!
```

Althea

```
!
hostname althea
!
enable password ######
!
username bertha password 7 094E5B1739522:       PPP username with encrypted display of password (“7
                                                  094E5B1739522”)
isdn switch-type basic-5ess                     :configures router for specific ISDN switch
interface Ethernet0
ip address 171.68.158.49 255.255.255.248
!
interface BRI0
ip address 171.68.158.26 255.255.255.248
encapsulation PPP                               :specifies PPP encapsulation for the interface
ppp authentication chap                         :specifies PPP CHAP authentication for the interface
```

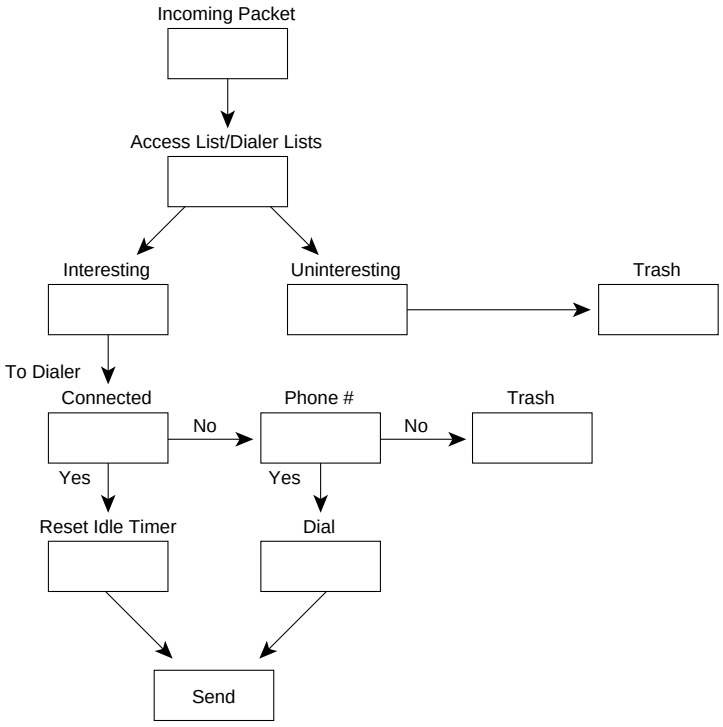
!

!

ISDN Implementation: Dial-on-Demand Routing

ISDN is implemented as a circuit-switched technology. Like the telephone network, ISDN connections are only made 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. Only if the packet is interesting will DDR bring up an ISDN link to communicate. Figure 4 is a diagram of the DDR process.

Figure 4. Dial-on-Demand Routing Process



ISDN Implementation: IP DDR Configuration

The sections that follow list the commands required for establishing an IP DDR connection over ISDN.

IP Addressing

IP addressing is done at the interface configuration level with the following commands:

- **ip address** <*ip address*> <*subnet mask*>

  This command assigns an IP address to the BRI interface.

  Note: The BRI interfaces of both routers must be on the same subnet.

- **ip unnumbered interface** <*lan interface*>

  This command can be used instead of the **ip address** command. It allows the BRI interface to use a LAN interface’s IP address as its own.

IP Routing

IP routing between sites can be handled via static routes, Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Enhanced IGRP, or Open Shortest Path First (OSPF). For simple configurations, static routes will be sufficient. The command for creating static routes is as follows:[4]

- **ip route** <*destination ip address*> <*destination ip subnet mask*> <*intermediate ip address*>

  The **ip route** command maps IP hosts and networks to an intermediate address. In this case all destinations available at the central site will be mapped to the central site BRI port's address (the intermediate address).

  Note: If the central site is running a routing protocol, the static routes from the remote site must be redistributed using the **redistribute static** router configuration command.

If desired, a routing protocol can be run instead of using static routes. The issue to remember is that each routing protocol will require sending regular updates, which in turn will cause the ISDN link to come up frequently. If RIP or IGRP are being used, the regular updates can be controlled using snapshot routing, a feature built into Cisco IOS software. If Enhanced IGRP or OSPF are being used, more creative methods will need to be employed in order to control routing updates across the link.

IP DDR Commands

Global Configuration Commands

- **dialer list** <*number*> **list** <*access list number*> or **dialer-list protocol** <*protocol*> **permit/deny/list**

  The Dialer-List command establishes access across the DDR link. A dialer list itself can permit or deny layer 3 traffic or it can call a more specific layer 2 or layer 3 access list. Following are two dialer list examples. The first is a generic statement that permits all IP traffic, while the second statement calls specific access lists (all access lists numbered 101).

```
Example 1:  Dialer-list 1 protocol ip permit
Example 2:  Dialer-list 1 list 101
            Access-list 101 permit ip any any
            Access-list 101 deny udp any any eq snmp
```

  The Dialer-List command works in conjunction with the Dialer-Group interface configuration command. The Dialer-Group command maps Dialer-List commands to a specific interface. The <number> that follows the DIALER LIST command serves as a reference number (for example, **dialer-list 1)**. To map this dialer list to a specific interface, the Dialer-Group command must call the same reference number **(dialer-group 1)**.

- **access-list** <*number*> **deny/permit** <*source number or source-wildcard*>

  Access lists allow traffic to be controlled based on network-layer filtering. Cisco offers standard access lists and extended access lists, both of which can be called by the **dialer-list** command. The above command refers to standard access lists. To indicate that the command is a standard IP access list, use a number between 1 and 99 for the access list number. Extended IP access lists user access list numbers between 100 and 199. For command information for extended access lists refer to Cisco Connection Documentation CD-ROM.

Interface Configuration Commands

- **dialer-group** <*dialer group number*>

---

4. Refer to Cisco documentation or Cisco Connection Documentation CD-ROM for information on configuring routing protocols.

This command assigns a dialer-group to the BRI interface. Based on the number used, the dialer group maps to one or more dialer list(s). As discussed, both the **dialer-group** and the **dialer-list** commands must be used. They serve as the foundation for DDR access over the ISDN line.

- **dialer map** *<ip> <destination ip address>* **name** *<destination router name>* **speed** *<speed of isdn link 56 or 64>* **[broadcast]** *<isdn phone number>*

  The **dialer map** command is the cornerstone for establishing a DDR link. The command maps a network address to an ISDN number. Note that the name that is used in the dialer map statement must also exist as a username with password on the local router. This is necessary for PPP CHAP authentication.

  The speed should be set to either 56 or 64. For the most part, if the ISDN source and destination reside off the same Central Office switch, the 64-kbps setting should work. If the ISDN source and destination reside off different switches and intraswitch communication is necessary, the 56-kbps setting should be selected.

  Note also the **broadcast** command. This command permits broadcast traffic to cross the ISDN link in addition to the regular unicast traffic that is permitted. The **broadcast** command is not necessary if static routes are being used. If RIP is in use, however, the broadcast statement is necessary in order for routing updates to cross the link.

  If the ISDN interfaces are configured using the **ip unnumbered** command, the destination IP address should be that of the same interface used by the **ip unnumbered** command.

IP Debugging Tools

When configuring and troubleshooting IP connections the following **debug** and **show** commands are useful:

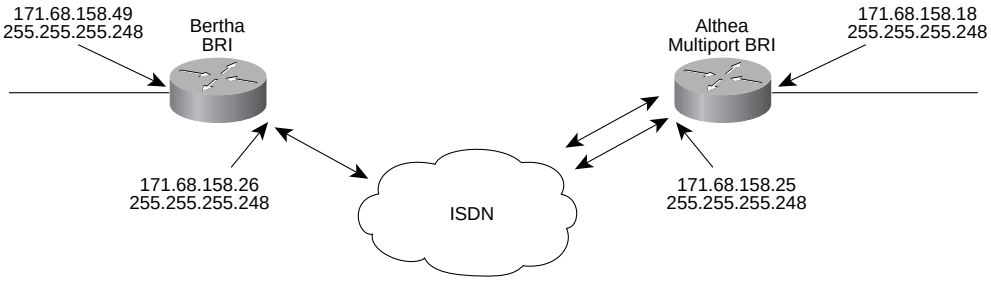
- debug ip packet
- debug ip tcp
- debug ip udp
- debug ip icmp
- debug ip routing
- show ip route
- show ip arp
- show ip traffic

Note: The **ping** command is also extremely used in troubleshooting DDR links. The default PING protocol is IP, although IPX and AppleTalk PING are also supported.

IP DDR Sample Configuration

In Figure 5, Bertha and Althea connect over ISDN via IP DDR.

Figure 5. Sample DDR Configuration



Bertha

```
!
hostname bertha
!
enable password ######
!
username althea password 7 094E5B1739522
isdn switch-type basic-5ess
interface Ethernet0
ip address 171.68.158.49 255.255.255.248
!
interface BRI0
ip address 171.68.158.26 255.255.255.248
encapsulation PPP
dialer map ip 171.68.158.25 name althea speed 56 14085551111
dialer-group 1
ppp authentication chap
!
ip route 131.108.0.0 255.255.0.0 171.68.158.25
ip route 171.69.0.0 255.255.0.0 171.68.158.25
access-list 101 permit ip any any
!
!
dialer-list 1 list 101
!
```

Althea

```
!
hostname althea
!
enable password ######
!
username bertha password 7 2394943E02B17
isdn switch-type basic-5ess
interface Ethernet0
```

```
ip address 171.68.158.18 255.255.255.248
!
interface BRI0
ip address 171.68.158.25 255.255.255.248
encapsulation PPP
dialer map ip 171.68.158.26 name bertha speed 56 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 list 101
!
```

ISDN Implementation: AppleTalk DDR Configuration

To add AppleTalk protocol support to the ISDN DDR link, follow the steps in the sections that follow.

AppleTalk Addressing

AppleTalk address configuration is performed in Interface configuration mode with the following commands:

- **appletalk cable-range** *<cable-range> <node address>*

  This command must be entered on both routers' ISDN interfaces, and the cable range must match on both ends. Additionally, for each router, manually assign the node address. See the configuration example later in this section.

- **appletalk zone** *<zone name>*

  This command must be entered on both routers. The zone name must be the same on both routers' ISDN interfaces. The remote LAN interface, however, should have a different zone name to reduce AppleTalk broadcasts across the link.

AppleTalk Routing

To enable AppleTalk routing on a Cisco router, enter the following global configuration command:

- appletalk routing

  This command enables AppleTalk routing on the router. The default routing protocol is the Routing Table Maintenance Protocol (RTMP), although AppleTalk Enhanced IGRP can be used instead by typing **appletalk routing eigrp***<at/eigrp router id>*. While Enhanced IGRP is an option, RTMP may make more sense in part because Enhanced IGRP sends out "hello" packets every 5 seconds, plus RTMP can be controlled via Snapshot Routing.

  Refer to the section on snapshot routing later in this document for managing routing updates over the ISDN link.

AppleTalk DDR Commands

The following are the basic commands required build AppleTalk DDR links.

Global Configuration Commands

- **dialer-list** <*number*> **protocol** <*appletalk*> **permit/deny** or **dialer-list** <*number*> **list** <*access list number*>

  Like with IP, the dialer list can be used in two different ways: to establish general protocol access or to call more specific access lists. Two dialer list examples follow; the first provides generic AppleTalk access, while the second calls a more specific access filter.[5]

```
Example 1:  Dialer-list 1 protocol AppleTalk permit

Example 2:  Dialer-list 1 list 601

            Access-list 601 permit other-access

            Access-list 601 deny cable-range 7100-7100
```

Interface Configuration Commands

- **dialer-group** <*dialer group number*>

  This command assigns a dialer group to the BRI interface. Based on the number used, the dialer group maps to one or more dialer list(s). As discussed, both the **dialer-group** and the **dialer-list** commands must be used. They serve as the foundation for DDR access over the ISDN line.

  Note: If all dialer-list statements use the same number (for example, Dialer-list 1...) then only one dialer-group statement is needed per interface.

- **dialer map** <*appletalk*> <*destination appletalk address*> **name** <*destination router name*> **speed** <*speed of isdn link 56 or 64*> **broadcast** <*isdn phone number*>

  This command maps an AppleTalk network address to an ISDN number.

  Note that the broadcast command is required in order for AppleTalk routing updates to cross the DDR link.

AppleTalk DDR Considerations

While AppleTalk over DDR works, a few problems can arise because of the nature of the AppleTalk protocol stack. The issue mainly revolves around licensing packets and Name Binding Protocol (NBP) lookups.

AppleShare 4.0, for example, sends out license management packets to ensure that the same copy is being run elsewhere. The license management packets are broadcast to each cable range, which will inherently include the ISDN links. An access list can be created, however, to make the license management packets “uninteresting” and therefore fail to bring up the ISDN DDR link.

The following command controls license management broadcast packets:

```
access list 601 permit includes <cable-range> broadcast-deny
```

This access list makes all traffic “interesting” for all networks/cable ranges, but it makes broadcasts “uninteresting.”

NBP packets can also cause excessive link uptime. 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 npb** command is useful in conjunction with the **debug dialer** command to monitor NBP traffic and DDR dialing causes.

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

---

5. Refer to Cisco Connection Documentation CD-ROM for additional information on AppleTalk access lists.

Cisco IOS Version 11.0 and later will offer NBP filter support that will help to control all zone NBP broadcasts. However, use the **NBP filter** command with caution. If NBP is used to link an application to other networked resources, a filter that blocks NBP traffic will ostensibly filter the network service.

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

AppleTalk Debugging

The following **debug** and **show** commands are useful for testing and troubleshooting AppleTalk connections:

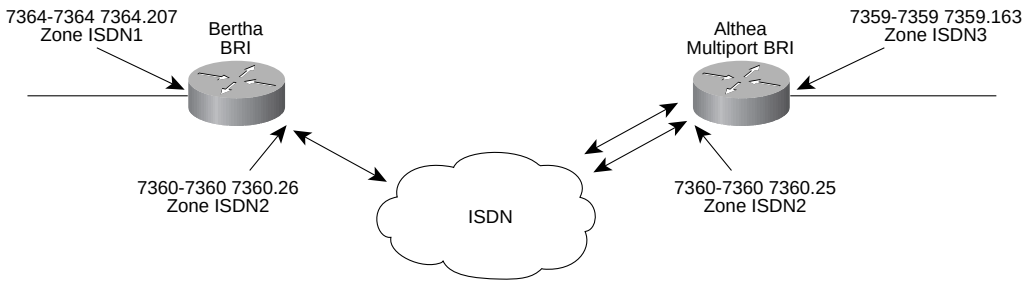
- debug apple packet [interface]
- debug apple nbp [interface]
- debug apple rtmp [interface]
- debug apple routing
- **show appletalk interface** <*interface*>
- show appletalk traffic
- show appletalk zone

Note: The **appletalk ping** command is also useful when troubleshooting AppleTalk DDR links.

AppleTalk DDR Sample Configuration

In Figure 6, Bertha and Althea connect over ISDN using AppleTalk DDR commands.

Figure 6. Sample AppleTalk DDR Configuration



Bertha

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

interface Ethernet0
ip address 171.68.158.49 255.255.255.248
AppleTalk cable-range 7364-7364 7364.207
AppleTalk zone ISDN1
!
interface BRI0
ip address 171.68.158.26 255.255.255.248
encapsulation PPP
AppleTalk cable-range 7360-7360 7360.26
AppleTalk zone ISDN2
dialer map ip 171.68.158.25 name althea speed 56 14085551111
dialer map AppleTalk 7360.25 name althea speed 56 broadcast 14085551111
dialer-group 1
ppp authentication chap
!
ip route 131.108.0.0 255.255.0.0 171.68.158.25
ip route 171.69.0.0 255.255.0.0 171.68.158.25
access-list 101 permit ip any any
!
!
dialer-list 1 list 101
dialer-list 1 protocol AppleTalk permit
!
```

Althea

```
!
hostname althea
!
enable password ######
!
username bertha password 7 2394943E02B17
AppleTalk routing
isdn switch-type basic-5ess

interface Ethernet0
ip address 171.68.158.18 255.255.255.248
AppleTalk cable-range 7359-7359 7359.163
AppleTalk zone ISDN3
!
interface BRI0
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 bertha speed 56 14085552222
dialer map AppleTalk 7360.26 name bertha speed 56 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 list 101
dialer-list 1 protocol AppleTalk permit
!
```

ISDN Implementation: IPX DDR Configuration

The steps necessary for configuring IPX DDR are described in the sections that follow.

IPX Addressing

- **ipx network** <*ipx network address*>

  This command must be entered on both routers. Both routers must have the same IPX network address on their respective BRI or PRI interfaces.

IPX Routing

- ipx routing

  This command enables IPX routing on the router. The default IPX routing protocol is RIP/Service Advertisement Protocol (SAP). Routers running Version 10.3 of the Cisco IOS software can run NetWare Link Services Protocol (NLSP) instead of RIP/SAP. Refer to the Cisco IOS Release 10.3 documentation or Cisco Connection Documentation CD-ROM for configuring NLSP. While NLSP has its advantages, it may make more sense 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 DDR Commands

Global Configuration Commands

- **dialer-list** <*number*> **protocol** <*ipx*> **permit/deny** or **dialer-list** <*number*> **list** <*access list number*>

  The dialer list can be used in two different manners: to establish general protocol access or to call more specific access lists. Following are two dialer list examples; the first provides generic IPX access, while the second calls a more specific access filter.

```
Example 1:  Dialer-list 1 protocol ipx permit

Example 2:  Dialer-list 1 list 901

            Access-list 901 permit -1 -1
```

Refer to Cisco Connection Documentation CD-ROM for more information on IPX access lists.

- **ipx route** <*destination IPX address*> <*intermediate IPX address*>

  This command works like the **ip route** command to create IPX static routes. This command is not necessary if a dynamic routing protocol is in use (for example, RIP/SAP or NLSP).

- **ipx sap** <*sap type*> <*sap service name*> <*ipx address*> <*socket number*> <*hop count*>

  This command creates a static SAP entry. This command is not necessary if a dynamic routing protocol is in use.

Interface Configuration Commands

- **dialer-group** <*dialer group number*>

  This command assigns a dialer group to the BRI interface. Based on the number used, the dialer group maps to one or more dialer-list(s). As discussed, both the **dialer-group** and the **dialer-list** commands must be used. They serve as the foundation for DDR access over the ISDN line.

  Note: If all dialer list statements use the same number (such as Dialer-list 1...), then only one dialer group statement is needed per interface.

- **dialer map** <*ipx*> <*destination ipx address*> **name** <*destination router name*> **speed** <*speed of isdn link 56 or 64*> **broadcast** <*isdn phone number*>

  This command maps an IPX network address to an ISDN number.

Note that the **broadcast** command is required in order for RIP/SAP routing updates to cross the DDR link.

- ipx watchdog-spoof

  This command is designed to reduce IPX traffic across the ISDN link. When enabled, watchdog packets are spoofed at the local router. This 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 uptime.

IPX Debugging

The following **debug** and **show** commands are useful for IPX DDR configuration and troubleshooting tasks:

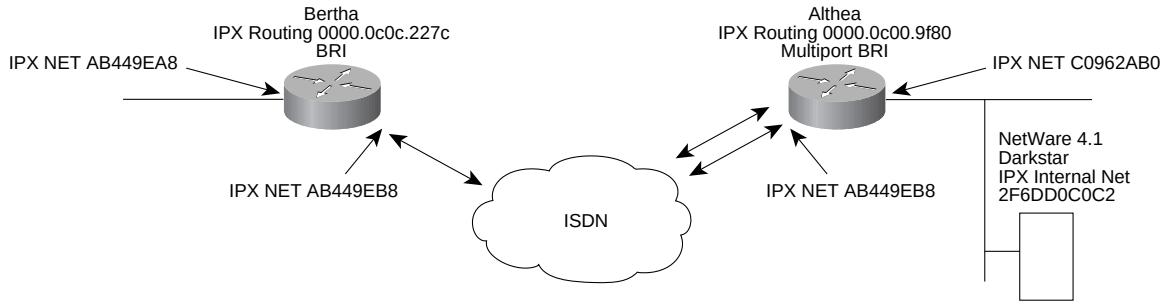
- debug ipx packet
- debug ipx routing
- debug ipx sap
- show ipx route
- show ipx servers
- show ipx traffic

Note: The **ipx ping** command is also useful when troubleshooting IPX DDR links.

IPX DDR Sample Configuration

In Figure 7, Bertha and Althea connect over ISDN using IPX DDR commands.

Figure 7. Sample IPX DDR Configuration



```
!
hostname bertha
!
enable password ######
!
username althea password 7 094E5B1739522
AppleTalk routing
ipx routing 0000.0c0c.227c
isdn switch-type basic-5ess


interface Ethernet0
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 ISDN1
!
interface BRI0
ip address 171.68.158.26 255.255.255.248
ipx network AB449EB8
ipx watchdog-spoof
encapsulation PPP
AppleTalk cable-range 7360-7360 7360.26
AppleTalk zone ISDN2
dialer map ip 171.68.158.25 name althea speed 56 14085551111
dialer map AppleTalk 7360.25 name althea speed 56 broadcast
  14085551111
dialer map IPX AB449EB8.0000.0c00.9f80 name althea speed 56
  broadcast 14085551111
dialer-group 1
ppp authentication chap
!
ip route 131.108.0.0 255.255.0.0 171.68.158.25
ip route 171.69.0.0 255.255.0.0 171.68.158.25
```

```
access-list 101 permit ip any any
!
ipx route 2FCB6448 AB449EB8.0000.0c00.9f80:optional             :optional
ipx route AB449EA0 AB449EB8.0000.0c00.9f80:optional             :optional
!
ipx sap 4 DARKSTAR 2F6DD0C0C2.0000.0000.0001 451 2              :optional
!
dialer-list 1 list 101
dialer-list 1 protocol AppleTalk permit
dialer-list 1 protocol novell permit
!
```

Althea

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

interface Ethernet0
ip address 171.68.158.49 255.255.255.248
ipx network C0962AB0
ipx encapsulation SAP
AppleTalk cable-range 7364-7364 7364.207
AppleTalk zone ISDN1
!
interface BRI0
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 althea speed 56 14085552222
dialer map AppleTalk 7360.25 name althea speed 56 broadcast 14085552222
dialer map IPX AB449EB8.0000.0c0c.227c name bertha speed 56 broadcast 14085552222
dialer-group 1
ppp authentication chap
!
ip route 131.108.0.0 255.255.0.0 171.68.158.25
ip route 171.69.0.0 255.255.0.0 171.68.158.25
access-list 101 permit ip any any
!
!
dialer-list 1 list 101
dialer-list 1 protocol AppleTalk permit
dialer-list 1 protocol novell permit
!
```

ISDN Implementation: Dial-Backup for Leased Lines

Cisco IOS Dial Backup Overview

The dial backup service provides protection against WAN downtime by allowing a dedicated serial connection to be backed up via a circuit-switched connection. To configure dial backup, simply associate a secondary interface (the ISDN interface in this case) as a backup to a primary serial interface.

Once configured, the dial backup software keeps the secondary line inactive until one of the following conditions is met:

- The primary line goes down.
- The transmitted traffic load on the primary line exceeds a defined limit.

In the first instance, when the software detects a lost Carrier Detect signal from the primary line device or when the line protocol is down, it activates the secondary line. At this point the ISDN line comes up, preserving the connection between the two sites.

In the second instance, the software monitors the traffic loads and computes a five-minute moving average. If the average exceeds the user-defined value for the line, the secondary line is activated. Depending on how the secondary line is configured, some or all of the traffic flows onto the secondary line.

A value can also be specified to define when the secondary line should be disabled and the amount of time the secondary line can take going up or down.

Dial-Backup Configuration Commands

There are three principal commands for establishing a dial backup service. The three commands are interface configuration commands that are applied to the primary line. If for example, the Serial 0 interface is to be backed up by an ISDN circuit, type **config terminal** then **interface serial 0** to enter the dial backup commands.

Interface Configuration Commands

- **backup interface** <*interface name*>

  This command assigns a particular interface to be a backup for a primary link. The interface name entered (for example, BRI 0) refers to the backup line.

- **backup load** <*enable threshold*> **never** <*disable load*> **never**

  With this command, the backup line is activated based on traffic thresholds on the primary link. The load refers to a percentage of the primary line's available bandwidth.

- **backup delay** <*enable delay*> **never** <*disable delay*> **never**

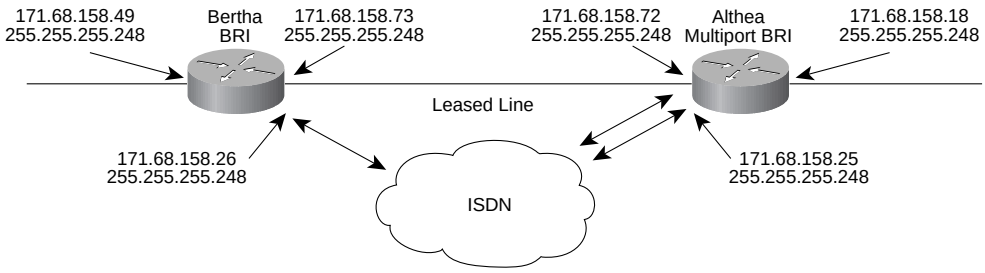
  The **backup delay** command defines how much time should elapse before a secondary line is set up or taken down (after a primary line transitions).

Following are sample configurations for dial backup with ISDN. For simplicity, IP is the only configured protocol, although other protocols could also be configured.

Dial-Backup Configuration Examples

In Figure 8, ISDN is used to back up the primary leased line facility that connects between Bertha and Althea.

Figure 8. Sample Dial-Backup Configuration



Example 1

The following example configures BRI 0 as a secondary line that activates only when the primary line (Serial 0) goes down. The backup delay command configures the backup connection to activate 30 seconds after the primary link goes down and to remain on for 60 seconds after the primary line is reactivated.

Bertha

```
!
hostname bertha
!
enable password ######
!
username althea password 7 094E5B1739522
isdn switch-type basic-5ess

interface Ethernet0
ip address 171.68.158.49 255.255.255.248
!
interface Serial0
ip address 171.68.158.73
backup interface BRI 0
backup delay 30 60
!
interface BRI0
ip address 171.68.158.26 255.255.255.248
encapsulation PPP
dialer map ip 171.68.158.25 name althea speed 56 14085551111
dialer-group 1
ppp authentication chap
!
ip route 131.108.0.0 255.255.0.0 171.68.158.25
ip route 171.69.0.0 255.255.0.0 171.68.158.25
access-list 101 permit ip any any
!
!
dialer-list 1 list 101
```

Example 2

In this example the ISDN line is only brought up when the load of the primary line reaches a certain threshold. The secondary line is not activated when the primary line goes down. Instead the secondary line is activated when the load on the primary line is greater than 75 percent of the primary's bandwidth. The secondary line is then brought down when the aggregate load between the primary and secondary lines fits within 5 percent of the primary bandwidth.

Bertha

```
!
hostname bertha
!
enable password ######
!
username althea password 7 094E5B1739522
isdn switch-type basic-5ess

interface Ethernet0
ip address 171.68.158.49 255.255.255.248
!
interface Serial0
ip address 171.68.158.73
backup interface BRI 0
backup load 75 5
!
interface BRI0
ip address 171.68.158.26 255.255.255.248
encapsulation PPP
dialer map ip 171.68.158.25 name althea speed 56 14085551111
dialer-group 1
ppp authentication chap
!
ip route 131.108.0.0 255.255.0.0 171.68.158.25
ip route 171.69.0.0 255.255.0.0 171.68.158.25
access-list 101 permit ip any any
!
!
dialer-list 1 list 101
!
```

Example 3

In this example the secondary line is configured to activate once traffic threshold on the primary line exceeds 25 percent. Once the aggregate load of the primary and secondary lines returns to within 5 percent of the primary bandwidth, the secondary line is deactivated. The secondary line waits 10 seconds after the primary goes down before activating, and remains active for 60 seconds after the primary returns and becomes active again.

Bertha

```
!
hostname bertha
!
enable password ######
!
username althea password 7 094E5B1739522
isdn switch-type basic-5ess

interface Ethernet0
ip address 171.68.158.49 255.255.255.248
!
interface Serial0
ip address 171.68.158.73
backup interface BRI 0
backup load 25 5
backup delay 10 60
!
interface BRI0
ip address 171.68.158.26 255.255.255.248
encapsulation PPP
dialer map ip 171.68.158.25 name althea speed 56 14085551111
dialer-group 1
ppp authentication chap
!
ip route 131.108.0.0 255.255.0.0 171.68.158.25
ip route 171.69.0.0 255.255.0.0 171.68.158.25
access-list 101 permit ip any any
!
!
dialer-list 1 list 101
!
```

ISDN Implementation: Bandwidth-on-Demand

Cisco IOS Bandwidth on Demand Overview

As discussed earlier, ISDN provides multiple data channels, either 2 B channels for BRI service (2B+D), 23 B channels for T1 PRI (23B+D), or 30 B channels for E1 PRI (30B+D). Normally with DDR, ISDN will only use one B channel to connect between sites. This means that the second B channel will be unused. The Cisco IOS software, however, offers a bandwidth-on-demand (BOD) feature that allows the second B channel to be used in conjunction with the first. This in turn doubles the bandwidth across the link, from 56/64 kbps to 112/128 kbps. This should not be confused with PPP Multilink, however. Both concepts are intended to increase bandwidth between sites, but the implementation differs. Moreover, the Cisco IOS software does not offer PPP Multilink at this time. This discussion will be limited strictly to Cisco's current BOD offering.

For a discussion of B-channel aggregation techniques, refer to Appendix B.

Bandwidth on Demand Configuration Steps

The **dialer load-threshold** command is an interface configuration command used for enabling BOD on a given interface. Below is the syntax for the command:

- **dialer load-threshold** <*load*>

  The load refers to the load beyond which the dialer will initiate another call to the destination. This argument is a number between 1 and 255.

Bandwidth on Demand Configuration Example

Following is an example of BOD. In this example, the second B channel is employed when the first B channel is half used. This is a protocol-independent command.

Bertha

```
!
hostname bertha
!
enable password ######
!
username bertha password 7 2394943E02B17
isdn switch-type basic-5ess
!
interface Ethernet0
ip address 171.68.158.49 255.255.255.248
!
interface BRI0
ip address 171.68.158.26 255.255.255.248
encapsulation PPP
dialer map ip 171.68.158.25 name althea speed 56 14085551111
dialer load-threshold 128
dialer-group 1
ppp authentication chap
!
ip route 131.108.0.0 255.255.0.0 171.68.158.25
ip route 171.69.0.0 255.255.0.0 171.68.158.25
access-list 101 permit ip any any
!
dialer-list 1 list 101
```

ISDN Implementation: Snapshot Routing

Snapshot Routing Overview

In all the preceding configurations, ISDN is deployed as a circuit-switched connection. As such, ISDN is billed, or tariffed, based on usage. Given this model, the goal is to minimize uptime or at least control what brings the link up or down. This becomes a particular challenge, especially when routing protocols are employed because of their need to send regular broadcasts containing routing information.

There are two principal ways to control routing updates. The first is to use static routes. With static routes, all routes are entered manually, obviating the need for a routing protocol and eliminating routing updates. Static routes are effective to a certain point. However, if there a lot of different routes, manually entering the routes can be rather tedious. The other option is to run a routing protocol instead of using static routes, but to let snapshot routing control the routing protocol's update intervals.

Snapshot routing has been available since Release 10.2 of the Cisco IOS software. With snapshot routing, user-defined parameters can be set to control routing updates across links. Currently snapshot routing supports the following distance-vector routing protocols:

Routing Protocols	LAN Protocols
IGRP	TCP/IP
RIP	TCP/IP
RIP/SAP	Novell IPX/SPX
RTMP	AppleTalk
RTP	Banyan VINES

Under normal circumstances, these routing protocols broadcast updates every 10 to 60 seconds. This means that the ISDN link is brought up every 10 to 60 seconds simply to announce routing information. From a cost perspective, this is unacceptable. Snapshot routing remedies this problem.

There are two components to snapshot routing: snapshot server and snapshot client. When configuring snapshot routing, one router is designated the client snapshot router, and one or more other routers are designated as snapshot server routers. The client router determines the frequency at which routing information is exchanged between routers.

With snapshot routing enable, routing information is exchanged during an active period. During the active period a client router dials all the remote server routers for which it has a snapshot dialer map defined in order to get routes from all the remote locations. The server router provides information about routes to each client router that calls.

At the end of the active period, the router takes a snapshot of the entries in the routing table. These entries remain frozen during a quiet period. At the end of the quiet period, another active period starts during which routing information is again exchanged.

When the router transitions from the quiet period to the active period, the line might not be available for a variety of reasons. For example, the line might be down or busy. If this happens, the router has to wait through another entire quiet period before it can update its routing table entries. This might be a problem if the quiet period is very long, for example, around 12 hours. To avoid having to wait through the quiet period, you can configure 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 a dial-up environment in which there are more remote sites than router interface lines. For example, PRI has 23 DS0s available, but there may be 46 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.

To configure snapshot routing, follow the interface steps below. Note that snapshot routing is enabled/disabled through interface configuration commands.

Snapshot Server Configuration

- **snapshot server** <*active time*> **[dialer]**

  The active time refers to the amount of time, in minutes, that routing updates are regularly exchanged between client and server routers. This can be any integer between 5 and 100. Typically, a 5-minute interval is sufficient. The dialer command is an optional command that allows the client router to dial up the server router in the absence of regular traffic. The dialer command should be used on DDR links.

- **dialer map snapshot** <*snapshot number*> **name** <*destination router name*> **speed** <*speed of ISDN link 56 or 64*> **broadcast** <*ISDN phone number*>

  This command is necessary for running snapshot over DDR links. The snapshot number is a unique number used to identify the dialer map. The rest of the commands are identical to the DDR commands discussed earlier in this document.

Snapshot Client Configuration

- **snapshot client** <*client active time*> <*quiet time*> **[suppress-statechange-updates] [dialer]**

  The active time refers to the amount of time, in minutes, that routing updates are regularly exchanged between client and server routers. This can be any integer between 5 and 100. Typically, a 5-minute interval is sufficient. The quiet time refers to the amount of time in minutes that the routing entries remain frozen and unchanged. Routes are not aged during the quiet period, so they remain in the routing table as if they were static entries. The quiet time can be an integer between 8 and 100000. The **suppress-statechange-updates** command disables the exchange of routing updates each time the line protocol goes from "down" to "up" or from "dialer spoofing" to "fully up." The dialer command is an optional command that allows the client router to dial up the server router in the absence of regular traffic. The dialer command should be used on DDR links.

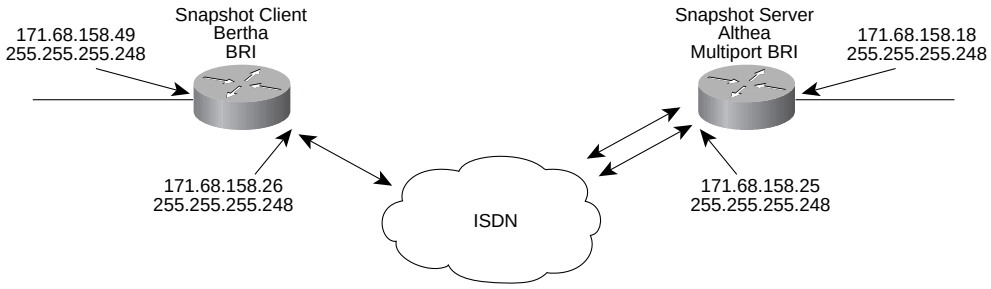
- **dialer map snapshot** <*snapshot number*> **name** <*destination router name*> **speed** <*speed of isdn link 56 or 64*> **broadcast** <*isdn phone number*>

  This command is necessary for running snapshot routing over DDR links. The snapshot number is a unique number used to identify the dialer map. The rest of the commands are identical to the DDR commands discussed earlier in this document.

Snapshot Configuration Examples

In the configuration shown in Figure 9, Althea is configured as a snapshot server router and Bertha is configured as a snapshot client. Note the dialer map statements that have been added for snapshot routing. In the example that follows, Bertha is configured for a 5-minute active period and a 480-minute quiet period. The **suppress-statechange-updates** command is also enabled.

Figure 9. Sample Snapshot Configurations



Bertha

```
!
hostname bertha
!
enable password ######
!
sername althea password 7 094E5B1739522
isdn switch-type basic-5ess

interface Ethernet0
ip address 171.68.158.49 255.255.255.248
!
interface BRI0
ip address 171.68.158.26 255.255.255.248
encapsulation PPP
dialer map ip 171.68.158.25 name althea speed 56 broadcast 14085551111
dialer map snapshot 1 name althea speed 56 broadcast 14085551111
dialer-group 1
snapshot client 5 480 suppress-statechange-updates dialer
ppp authentication chap
!
router rip
network 171.68.0.0
!
access-list 101 permit ip any any
!
!
dialer-list 1 list 101
!
```

Althea

```
hostname althea
!
enable password ######
!
```

```
username bertha password 7 2394943E02B17
isdn switch-type basic-5ess
!
interface Ethernet0
ip address 171.68.158.18 255.255.255.248
!
interface BRI0
ip address 171.68.158.25 255.255.255.248
encapsulation PPP
dialer map ip 171.68.158.26 name bertha speed 56 14085552222
dialer map snapshot 1 name bertha speed 56 broadcast 14085552222
dialer-group 1
snapshot server 5 dialer
ppp authentication chap
!
router rip
network 171.68.0.0
!
access-list 101 permit ip any any
!
!
dialer-list 1 list 101
!
```

ISDN Implementation: SNMP Management of ISDN

Cisco ISDN MIBs

At present there is no industry-standard ISDN management information base (MIB). However, as of Release 10.3(2) of the Cisco IOS software, two Cisco 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 first of the two MIBs is the Cisco ISDN MIB. This MIB focuses primarily on the ISDN interface and neighbor information. Currently two MIB groups are defined: demandNbrTable and demandNbrEntry. Table 2 shows an example of some of the MIB variables available under the ISDN MIB.

Table 2. Cisco ISDN MIB Variables

MIB Object	Description
demandNbrPhysIf	ifIndex 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

Table 2. Cisco ISDN MIB Variables

MIB Object	Description
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 router has refused

The second of the two Cisco ISDN MIBs is the Cisco Call History MIB. The MIB is intended to store call information for accounting purposes. The goal is to provide a historical view of an ISDN interface; how many calls have been placed, how long the calls were, etc. The majority of the call history MIB variables fall under the ciscoCallHistory MIB group. Table 3 shows an example of some of the MIB variables available.

Table 3. Cisco Call History MIB Variables

MIB Object	Description
ciscoCallHistoryStartTime	The value of sysUpTime when this call history entry was created; this is useful for a management station to retrieve all calls after a specific time
ciscoCallHistoryCalledNumber	The number this call is connected to
ciscoCallHistoryCallConnectionTime	The value of sysUpTime when the call was connected
ciscoCallHistoryCallDisconnectTime	The value of sysUpTime when the call got 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 uptime, which is useful for tracking ISDN charges.

Working with SNMP over ISDN

SNMP is a common protocol used for network management purposes. While the protocol has its benefits, it can cause excessive uptime for ISDN links as a result of recurring pollings by the SNMP management platform. HP OpenView, for example, will regularly poll the network for SNMP events. While this is how OpenView gathers its information, it can cause the ISDN links to be brought up and down frequently in order to check that the remote routers are there. Ultimately this results in higher ISDN usage charges.

In an effort to curb ISDN charges, filtering SNMP packets at the central site is recommended. The net effect is that SNMP packets destined to remote sites over ISDN are filtered out. Incoming SNMP packets, however, are still permitted, allowing SNMP traps to make it to the SNMP management platform. This is important because if a SNMP device fails at the remote site, the alarm is not filtered out.

Creating a filter for SNMP is done by creating an access list that denies SNMP traffic. An example of SNMP filtering follows. Note that two access lists have been created for SNMP filtering; this is because the layer 3 protocol for SNMP can be either IP or UDP. In the event that IPX SNMP is employed, a separate access list must be created.

Bertha

```
!
hostname bertha
!
enable password ######
!
username althea password 7 094E5B1739522
isdn switch-type basic-5ess

interface Ethernet0
ip address 171.68.158.49 255.255.255.248
!
interface BRI0
ip address 171.68.158.26 255.255.255.248
encapsulation PPP
dialer map ip 171.68.158.25 name althea speed 56 14085551111
dialer-group 1
ppp authentication chap
!
ip route 131.108.0.0 255.255.0.0 171.68.158.25
ip route 171.69.0.0 255.255.0.0 171.68.158.25
access-list 101 permit ip any any
access-list 101 deny tcp any any eq 161
access-list 101 deny udp any any eq snmp
!
!
dialer-list 1 list 101
!
```

ISDN Implementation: Advanced Topics

Cisco 7010/7000 T1/E1 MIP Controller Configuration for PRI

To configure ISDN PRI using the T1 MIP Controller, first perform the following global configuration command:

- **isdn switch-type** *<switch-type>*

  The Cisco IOS software supports a variety of ISDN switch types. To examine the supported switches, type **isdn switch-type ?** . An ISDN switch type must be specified. The switch type refers to the switch that the CO is using. Consult your carrier to find out which switch it is using. Note that in most cases this will be country specific.

Next, configure the MIP controller by first entering the **controller t1** <slot/port> command. The slot refers to the slot number on the Cisco 7010 or 7000 where the MIP controller has been installed. At this point enter the following controller configuration commands:

- **framing esf**

  This command sets the T1 framing to ESF or Extended Super Frame.

- linecode b8zs

  This command sets the line code to Bipolar 8 Zero Substitution.

- **pri-group** *<timeslots range>*

  If no timeslots are set, the specified controller defaults to 23 B channels and 1 D channel for T1 links.

The **pri-group timeslots** command establishes channels 1 through 23 as B channels and channel 24 for the D channel. The command also creates an interface called “interface serial <slot # of MIP card>/<interface # on MIP card>:23.” This interface can be configured with network protocol information and DDR information. Refer to the configuration that follows for a sample configuration using the MIP card for T1 PRI service.

```
Using 3390 out of 130048 bytes
!
version 10.3
service password-encryption
!
hostname Prometheus
!
enable password 7 110B0B0A1C1705
!
username Zeus password 7 030649040D0A2F
username Daedalus password 7 000601090F5E05
username Neptune password 7 08235E41021C0B
username all
ipx routing 0000.0c35.eded
appletalk routing
isdn switch-type primary-4ess
!
controller T1 2/0
    framing esf
    linecode b8zs
    pri-group timeslots 1-24
!
```

```
interface Ethernet1/0
    ip address 192.150.42.178 255.255.255.248
    ipx network C0962AB0
    ipx encapsulation SAP
    appletalk cable-range 7351-7351 7351.130
    appletalk zone Marketing Lab
!
interface Serial2/0:23
    ip address 171.68.158.185 255.255.255.248
    encapsulation ppp
    ipx network AB449EB8
    no ipx route-cache
    ipx watchdog-spoof
    appletalk cable-range 7375-7375 7375.25
    appletalk zone Mkt Lab ISDN1
    dialer idle-timeout 90
    dialer map appletalk 7375.15 name Daedalus speed 56 broadcast 4085770322
    dialer map ipx AB449EB8.0000.0c3b.a241 name Neptune speed 56 broadcast 41532571 40
    dialer map appletalk 7375.20 name Zeus speed 56 broadcast 4085771903
    dialer map ip 171.68.158.186 name Zeus speed 56 4085771903
    dialer map ip 171.68.158.187 name Daedalus speed 56 4085770322
    dialer map ip 171.68.158.188 name Neptune speed 56 4153257140
    dialer map snapshot 1 name Daedalus speed 56 broadcast 4085770322
    dialer map snapshot 1 name Zeus speed 56 broadcast 4085771903
    dialer map snapshot 1 name Neptune speed 56 broadcast 4153257140
    dialer map ipx AB449EB8.0000.0c0c.227c name Daedalus speed 56 broadcast 4085770 322
    dialer map appletalk 7375.30 name Neptune speed 56 broadcast 4153257140
    dialer map ipx AB449EB8.0000.0c0a.0e70 name Zeus speed 56 broadcast 4085771903
    dialer load-threshold 128
    dialer-group 1
    snapshot server 5 dialer
    ppp authentication chap
```

To check the status of the T1 controller, the following **show** command is useful:

- **show controllers t1** *<slot/port>*

To configure ISDN PRI using the E1 MIP controller, first perform the following global configuration command:

- **isdn switch-type** <*switch-type*>

  The Cisco IOS software supports a variety of ISDN switch types. To examine the supported switches, type **isdn switch-type ?** . An ISDN switch type must be specified. The switch type refers to the switch that the CO is using. Consult your carrier to find out which switch it is using. Note that in most cases this will be country specific.

Next, configure the MIP controller by first entering the **controller e1** <*slot/port*> command. The slot refers to the slot number on the Cisco 7010 or 7000 where the MIP controller has been installed. At this point enter the following controller configuration commands:

- framing crc4

  This command sets the T1 framing to CRC4.

- linecode hdb3

  This command sets the line code to High-Density Bipolar 3.

- **pri-group** <*timeslots range*>

  If no timeslots are set, the specified controller defaults to 30 B channels and 1 D channel.

The **pri-group timeslots** command will establish channels 1 through 15 and 17 through 31 as B channels and channel 16 for the D channel. The command will also create an interface called “interface serial <slot # of MIP card>/<interface # on MIP card>:16.” This interface can then be configured with network protocol information and DDR information. Refer to the sample configuration that follows for an example of using the MIP card for E1 PRI service.

```
Using 3390 out of 130048 bytes
!
version 10.3
service password-encryption
!
hostname Prometheus
!
enable password 7 110B0B0A1C1705
!
username Zeus password 7 030649040D0A2F
username Daedalus password 7 000601090F5E05
username Neptune password 7 08235E41021C0B
username all
ipx routing 0000.0c35.eded
appletalk routing
isdn switch-type primary-net5
!
controller E1 2/0
     framing crc4
     linecode hdb3
     pri-group timeslots 1-31
!
```

```
interface Ethernet1/0
      ip address 192.150.42.178 255.255.255.248
      ipx network C0962AB0
      ipx encapsulation SAP
      appletalk cable-range 7351-7351 7351.130
      appletalk zone Marketing Lab
!
interface Serial2/0:16
      ip address 171.68.158.185 255.255.255.248
      encapsulation ppp
      ipx network AB449EB8
      no ipx route-cache
      ipx watchdog-spoof
      appletalk cable-range 7375-7375 7375.25
      appletalk zone Mkt Lab ISDN1
      dialer idle-timeout 90
      dialer map appletalk 7375.15 name Daedalus speed 56 broadcast 4085770322
      dialer map ipx AB449EB8.0000.0c3b.a241 name Neptune speed 56 broadcast 4153257140
      dialer map appletalk 7375.20 name Zeus speed 56 broadcast 4085771903
      dialer map ip 171.68.158.186 name Zeus speed 56 4085771903
      dialer map ip 171.68.158.187 name Daedalus speed 56 4085770322
      dialer map ip 171.68.158.188 name Neptune speed 56 4153257140
      dialer map snapshot 1 name Daedalus speed 56 broadcast 4085770322
      dialer map snapshot 1 name Zeus speed 56 broadcast 4085771903
      dialer map snapshot 1 name Neptune speed 56 broadcast 4153257140
      dialer map ipx AB449EB8.0000.0c0c.227c name Daedalus speed 56 broadcast 4085770322
      dialer map appletalk 7375.30 name Neptune speed 56 broadcast 4153257140
      dialer map ipx AB449EB8.0000.0c0a.0e70 name Zeus speed 56 broadcast 4085771903
      dialer load-threshold 128
      dialer-group 1
      snapshot server 5 dialer
      ppp authentication chap
```

To check the status of the E1 controller, the following **show** command is useful:

`show controllers e1` <*slot/port*>

Check layer 1 of the PRI over E1.

Aggregating BRI Interfaces

Using the **rotary-group** command, it is possible to aggregate multiple BRI interfaces. In doing so, two sites can gain greater bandwidth using ISDN. Similar to the **dialer load-threshold** command that aggregates the two B channels, the **rotary-group** command aggregates multiple BRI interfaces. To perform this operation, map BRI interfaces to a dialer interface using **dialer rotary-group.** Next, use the **interface dialer** command to create a dialer interface. Use **interface dialer** for assigning network addresses and creating dialer map statements. The **dialer load-threshold** command can be used in conjunction with the **dialer rotary-group** command to bring up multiple ISDN BRIs based on traffic thresholds. The **dialer load-threshold** command should be part of the **interface dialer** configuration.

A sample configuration follows:

```
!
int bri 0
dialer rotary-group 1
int bri 2
dialer rotary-group 1
int dialer 1
ip address 3.3.3.3 255.255.255.0
dialer map ip 3.3.3.4 name icarus speed 56 4085551212
!
```

ISDN Security

Calling Line Identification Screening

This command applies on Cisco routers that have BRI interfaces. Calling Line Identification (CLI), also called CallerID, screening adds a level of security by allowing a router to screen incoming calls. With CLI screening enabled, incoming calls can be verified to ensure that came from an expected origin. Note that CLI screening must be supported on the CO switch in order for the router to receive CLI information. Note also that CLI screening is configured but not supported by the CO switch; the router will reject all calls.

To configure CLI screening, enter the following interface configuration command:

- **isdn caller [number]**

Called Party Number Verification

When multiple devices are attached to an ISDN BRI, you can ensure that only a single device answers an incoming call by verifying the number or subaddress of the incoming call against the device's configured number or subaddress or both.

The router can be configured to verify a called-party number or subaddress number in the incoming setup message for ISDN BRI calls if the number is delivered by the switch.

To configure Called Party Number Verification, enter the following interface configuration command:

- **isdn answer1** [called-party-number] [:subaddress]

Verifying the called party number ensures that only the desired router responds to an incoming call. To configure a second number to be allowed, perform the following interface configuration command:

- **isdn answer2** [called-party-number] [:subaddress]

Without the **isdn answer** command, all calls are processed/accepted.

IP Enhanced IGRP and ISDN

The Enhanced IGRP routing protocol sends out “hello” packets every 5 seconds to maintain its routing tables. While this is acceptable on LAN links, it is not as desirable for ISDN links. For all intents and purposes, the link would never go down.

Currently, the Cisco IOS snapshot routing feature does not support the Enhanced IGRP routing protocol. As a result, routers running Enhanced IGRP have to resort to other techniques to control Enhanced IGRP routing updates across the ISDN links. Below are three solutions to address Enhanced IGRP traffic over ISDN.

1. Use the **passive-interface** router configuration command to declare the ISDN interface passive. With the passive interface command applied to an ISDN interface, Enhanced IGRP excludes the ISDN interface when it broadcasts routing updates. This in turn prevents the ISDN line from coming up. If the passive interface command is used, use static routes to build connections across the ISDN link.

   To set the interface to passive, first enter router configuration by typing **router eigrp** <Autonomous System>. Next, type **passive-interface** <interface> to declare the interface passive.

   In the following sample configuration, the ISDN BRI 0 interface is set to passive:

```
!
router eigrp 203
network 171.68.158.0
passive-interface BRI 0
!
```

2. Access lists are another way of controlling Enhanced IGRP traffic. Specifically, two access lists can be created:

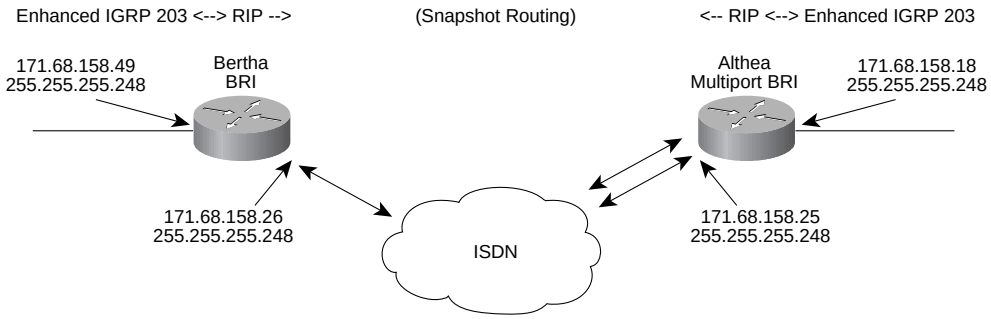
```
access-list 101 deny eigrp any any
access-list 101 deny ip any 224.0.0.10 0.0.0.0\
```

   The first access list denies all Enhanced IGRP traffic, while the second specifically denies the multicast address 224.0.0.10, the multicast address that Enhanced IGRP uses for its updates. To apply these access lists to an ISDN interface, remember to have a dialer list in global configuration mode that maps the preceding two access lists (that is, dialer list 1 list 101). Additionally, a **dialer-group** command must exist mapping the dialer list to the ISDN interface. As with the passive interface command, filtering out Enhanced IGRP will require that static routes be used to create routes across the ISDN link.

3. Using the RIP routing protocol is another way to handle ISDN links in Enhanced IGRP-based designs. Essentially, use Enhanced IGRP for the entire network except the ISDN links. For the ISDN links, configure RIP and then let snapshot routing control the RIP updates across the ISDN link. In order for this approach to work, the RIP information must be redistributed into the Enhanced IGRP networks and vice versa.

Figure 10 depicts a simple network design in which Enhanced IGRP is used on both LANs, while RIP runs in between the two sites.

Figure 10. RIP Solution for Enhanced IGRP-Based Networks



Bertha

```
!
router eigrp 203
network 171.68.0.0
redistribute rip
passive interface interface bri 0
!
router rip
network 171.68.0.0
redistribute eigrp 203
passive interface interface eth 0
!
```

Althea

```
!
router eigrp 203
network 171.68.0.0
redistribute rip
passive interface int bri 0
!
router rip
network 171.68.0.0
redistribute eigrp 203
passive interface int eth 0
!
```

Note: There is a risk of feedback loops with this approach, because routes redistributed into Enhanced IGRP from RIP can potentially be redistributed back into RIP. To avoid this, use the **distribute-list** command for RIP and Enhanced IGRP to control which routes are passed back and forth.

Note: Default metrics may also need to be added when redistributing one routing protocol into another. Refer to Cisco Connection Documentation CD-ROM for information about default metric settings.

ISDN Implementation: Latest Cisco IOS Enhancements

With each new release of the Cisco IOS software, new features relating to ISDN are added.

The following are ISDN feature enhancements in Cisco IOS Release 10.3:

- PPP software compression for ISDN

- ISDN Primary Rate Interface signaling software for Europe and Australia
- Support for VINES, OSI, and DECnet IV over ISDN
- Fast failover for ISDN
- LAPB encapsulation for DDR links
- Semipermanent connections for German 1TR6 ISDN
- Frame Relay over ISDN

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. PPP CCP allows vendors to support multiple data compression algorithms. The Cisco implementation supports the STAC and Predictor algorithm options. Compression with ISDN will provided increased throughput and shorter file transfer times while reducing latency and improving real-time response.

An E1 version of the Multichannel Interface Processor (MIP) card is now available. This card can be used as an ISDN PRI when used in conjunction with the ISDN PRI signaling software available in Cisco IOS Release 10.3. Initially the ISDN PRI signaling provides support for I.421 Euro-ISDN signaling in Europe. This support will be enhanced to cover TS014 signaling for Australia in a 10.3 Maintenance Release.

Release 10.3 also introduces VINES, OSI, and DECnet IV support. Access lists for these protocols can be used to define “interesting” packets (packets that will trigger the DDR link). Also introduced is support for IPX floating static routes. The administrative distance of an IPX floating static route can be configured so that this route is less desirable than a dynamic route. If the dynamic route is lost, the floating static route can take over, and traffic can be sent through this alternative route. If this alternative route is provided by an ISDN interface, ISDN can be used as a backup mechanism.

Fast Failover of ISDN is intended for sites that have multiple ISDN numbers assigned to a single network destination address at their ISDN hub sites. A Cisco router can be configured to dial these numbers sequentially in an attempt to find a free B channel. Fast Failover for ISDN allows multiple ISDN numbers to be assigned to a single network destination address, with very fast dialing of a second or subsequent number in the event that the initial call fails.

Support has also been added for Link Access Procedure, Balanced (LAPB) encapsulation over ISDN DDR links with Release 10.3. Prior to Release 10.3, support was only offered for PPP, HDLC, and X.25. The addition of LAPB support enables the use of features that rely on this transport mechanism.

The last two features (ISDN semipermanent connections and Frame Relay over ISDN) will be offered with the 10.3(2) Maintenance Release. An ISDN semipermanent connection is a circuit-switched connection which, after being set up, will not be released for an agreed-upon subscription period. It can be viewed as a “nailed up” connection that is routed via the normal Telco ISDN network. ISDN semipermanent connections offer cost savings over normal ISDN circuit-switched connections to users who are willing to commit themselves to agreed-upon subscription periods. This feature is provided as part of the German national 1TR6 ISDN signaling system, and as such, is only applicable to markets that support this form of D-channel signaling.

Finally, Frame Relay over ISDN support will enable the router to send Frame Relay traffic over an ISDN network to a Frame Relay network using Frame Relay encapsulation over the ISDN network. This feature can be used either for basic access to Frame Relay services via an ISDN network or for backup of Frame Relay PVCs with an ISDN connection.

Future Cisco IOS Enhancements for ISDN

The following features are planned for Cisco IOS Release 11.0.

AppleTalk NBP Filtering

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. AppleTalk NBP filtering allows Cisco routers to build firewalls, dial-on-demand triggers, and queuing options based on any NBP type or object.

SPX Spoofing

Some Sequenced Packet Exchange (SPX)-based services in a Novell environment use SPX watchdog 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 will receive, recognize, and successfully acknowledge these watchdog packets both at the server end and the client end.

ISDN Fast Switching

To date, all ISDN WAN connectivity has been process switched. While this is not a disadvantage when dealing with a single BRI interface, the introduction of MBRI and PRI interfaces has introduced some performance limitations when fully loaded across all B channels. Fast Switching removes the performance limitations.

Callback for ISDN/DDR

Callback for ISDN/DDR enables a Cisco router using a DDR interface and PPP encapsulation to initiate a circuit-switched WAN link to another device and request that it be called back. In addition to PPP, the process uses the facilities specified in RFC 1570 (PPP LCP callback request). Callback for ISDN/DDR is particularly useful for sites that want to centralize billing. It also allows organizations to take advantage of disparities in tariffing on both a national and an international basis.

APPENDIX A: ISDN Technology Overview

The Basics

The two most common ISDN services are Basic Rate Interface (BRI) and Primary Rate Interface (PRI). The main difference between the two services is the number of available channels. From the local loop perspective, ISDN carries digital signals between the two points. The ISDN service comprises several logical channels for signaling and user data. The logical channels coexist using time division multiplexing (TDM). With TDM, each channel has a dedicated time slot on the link. Transmission is an aggregate of the time slots.

There are three basic types of channels: D, B, and H.

- *D channel*: Carries signaling between the user and the network. It can also be configured to carry data. Operates at either 16 kbps or 64 kbps.
- *B channel*: Carries information for user services, including voice, video, and other digital data. Operates at 64 kbps.
- *H channel*: Same function as B channel but operates at speeds greater than DS0 (64 kbps).

While all ISDN devices attached to the network using a standard physical connector and exchanging similar messages, the content of the service in use can vary. An ISDN telephone, for example, will request different services from the network than will a high-speed file transfer. The protocols used for different ISDN services are standardized and are sent using the D channel.

With the D channel used for signaling to the network, this leaves the B channel free to exchange user data such as voice and video. B channels always operate at 64 kbps, the bit rate required to digitize voice using PCM (Pulse Code Modulation). The B channel can be used for both circuit-switched and packet-switched applications. Note that in some cases, the B channel may be rate adapted to 56 kbps.

If a network service requires a bit rate higher than the B-channel offering, an H channel can be used instead. The first H channel is an H_0 channel with a data rate of 384 kbps or the equivalent of six B channels. An H_1 channel comprises all available H_0 channels at a single-user interface employing a T1 or E1 carrier. An H_{11} channel operates at 1.536 Mbps (T1 compatible) and is equivalent to four H_0 channels (24 B channels). Finally, an H_{12} channel operates at 1.920 Mbps (E1 compatible) and is equivalent to five H_0 channels (30 B channels).

ISDN Interfaces

The ISDN BRI interface comprises two B channels and one D channel. BRI is often expressed as 2B+D. In this case, the D channel operates at 16 kbps. BRI service is most commonly used in one of two ways. The first method connects end users (residential or business customers) to the Central Office (CO) via the local loop. The other method connects end users to an ISDN-compatible PBX.

The ISDN PRI interface has a number of different configurations. In North America and Japan, PRI service is designated as 23B+D, or 23 B channels and 1 D channel operating at 64 kbps. Alternatively, the PRI can be configured as 24B, in which case the D channel is defined on another. PRI also defines 30B+D, based upon E1 carrier facilities.

ISDN Devices

The ISDN CO is called the local exchange (LE). ISDN protocols are implemented in the LE, which is also considered the network side of the ISDN local loop. Some ISDN CO switch manufacturers break down the LE into local termination (LT) and exchange termination (ET). The LT handles functions associated with the termination of the local loop, while the ET is responsible for switching functions.

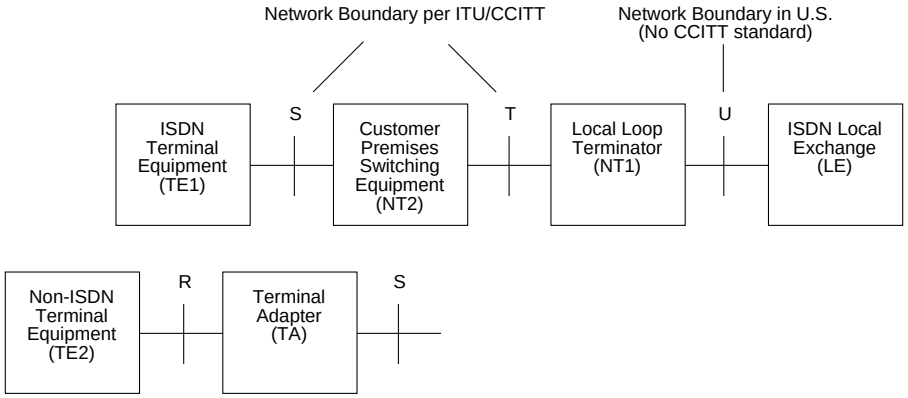
At the customer site, the ISDN local loop is terminated using a network termination type 1 (NT1). The NT1's responsibilities include line performance monitoring, timing, physical signaling protocol conversion, power transfer, and the multiplexing of the B and D channels.

ISDN also prescribes a network termination type 2 (NT2). NT2 devices are responsible for customer site switching, multiplexing, and concentration. PBXs, LANs, mainframe computers, terminal controllers, and other customer premises equipment (CPE) for voice and data switching can be considered NT2 equipment. In residential or Centrex environments, NT2 equipment is absent.

There are two other notable ISDN devices: terminal equipment (TE) and terminal adapters (TA). TE refers to end-user devices such as digital telephones or workstations. Native ISDN terminals are referred to as terminal equipment type 1 (TE1). Non-ISDN terminals such as DTE that predate the ISDN standards are referred to as terminal equipment type 2 (TE2). TE1s connect to the ISDN network through a four-wire, twisted-pair digital link. TE2s connect to the ISDN network through terminal adapters. The ISDN TA can either be a standalone device or a board inside the TE2. If the TE2 is implemented as a standalone device, it connects to the TA via a standard physical-layer interface. Examples include EIA/TIA-232-C (formerly RS-232-C), V.24, and V.35. The TA performs the necessary protocol conversion to allow non-ISDN (TE2) equipment to access the ISDN network.

Note the use of reference points R, S, T, and U as shown in Figure 11. As depicted, the R reference point is between non-ISDN terminal equipment (TE2) and a TA. The TA allows the TE2 to appear to the network as an ISDN device. There is no standard for the R reference point. Vendors can choose a variety of different physical connections and communication schemes.

Figure 11. ISDN Devices and Reference Points



The S reference point lies between ISDN user equipment: between the TE1 or TA and the NT2 or NT1. The T reference point is between the customer site switching equipment (NT2) and the local loop termination (NT1). The International Telecommunications Union (ITU) (formerly International Telegraph and Telephone Consultative Committee (CCITT)) specifically addresses protocols for the S and T reference points. In the absence of NT2 equipment, the user-network interface is usually called the S/T reference point.

Transmission between the NT1 and the LE occurs at the U reference point. The ITU considers the physical NT1 device to be owned by the network administration. That makes the entire local loop part of the network. The Federal Communications Commission (FCC) views the model differently. According to the FCC, since the NT1 resides on the customer premises it is considered CPE. Consequently, the user-network boundary exists at the LE, and the U reference point serves as the separator.

ISDN LE Equipment

There are several companies that manufacture ISDN-compatible network switches. Recall that the ISDN LE functions can be subdivided into two categories, LT and ET. The LT function primarily deals with the transmission facility and termination of the local loop. The ET functions deals with the switching portion of the LE. First the ET 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.

Today, there are two principal ISDN switches in the United States and Canada: AT&T's 5ESS and Northern Telecom's DMS-100. Until the current release of National ISDN-1 software, incompatibility between the AT&T and NT switches meant, for example, that AT&T ISDN telephone sets could not be used with an NT switch.

There are roughly 1600 5ESS switches 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 CO. The 5ESS was first put into service in 1982 and is capable of serving up to 100,000 local loops.

The Northern Telecom 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.

While AT&T and Northern Telecom remain the dominant switch manufacturers, there are other ISDN switches. Other ISDN switches include the following:

- Alcatel 1210
- Ericsson AXE 10
- Fujitsu FETEX-150
- Mitel GX5000 Global Switch
- NEX America NEAX 61A and 61E
- Siemens Stromberg-Carlson EWSD (Elektronisches Wahl System Digital)

In other parts of the world, ISDN switches are country specific. Table 4 lists countries and the ISDN switches that they employ.

Table 4. Countries and ISDN Switches Used

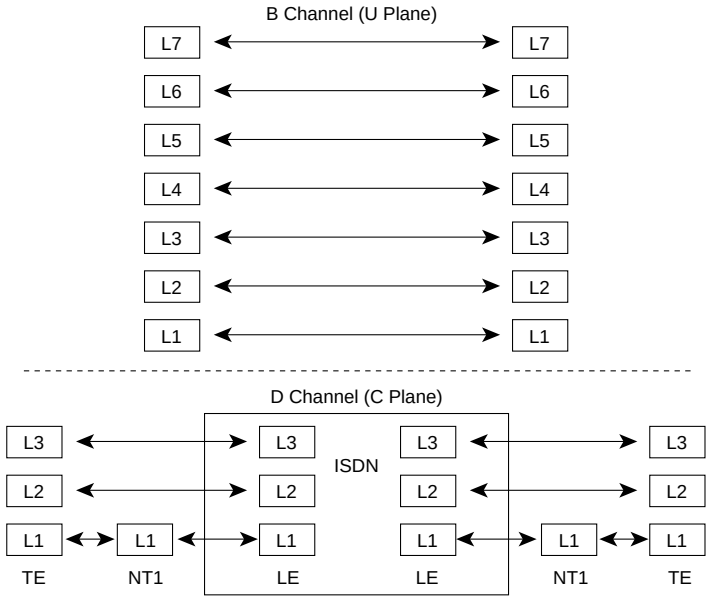
Country	Switch Type
Australia	basic-ts013
France	vn2
	vn3
Germany	basic-1tr6
Japan	ntt
	primary-ntt
Norway	basic-nwnet3
U.K.	basic-net3
	primary-net5

ISDN BRI Protocol Architecture

The ISDN protocol architecture is best understood by employing a two-plane model: one plane for signaling and one plane for user information. The ITU has introduced the concept of a control plane (C plane) and a user plane (U plane). Protocols within the C plane deal with the call establishment, call control, call termination, and other service requests. The U-plane protocols, on the other hand, handle the transfer of user information such as digitized voice and video between end-user applications.

Figure 12 shows a schematic for ISDN.

Figure 12. ISDN Schematic Drawing



The bulk of ISDN protocols address the user-network interface or signaling over the D channel. This corresponds to the C plane. The D channels are roughly equivalent to the lower three layers of the OSI reference model. Because these protocols describe only the user-network interface and no user-to-user communications, there are no D-channel counterparts for the OSI end-to-end layers.

The three protocol layers for the D channel are as follows:

- *Layer 1* Describes the physical connection between the TE, the NT, and the LE. Layer 1 includes specifications for the connector, line coding scheme, framing, and electrical characteristics. The physical connection is synchronous, serial, and full duplex. Additionally the connection may be point-to-point (PRI or BRI) or point-to-multipoint (BRI only). The D and B channels share the physical line using TDM.
- *Layer 2* Describes the procedures to ensure error-free communication over the physical link and defines the logical connection between the user and the network. The protocol also provides the rules for multiplexing multiple TEs on a single physical channel (multipoint).
- *Layer 3* Defines the user-network interface and signaling messages used to request services from the network.

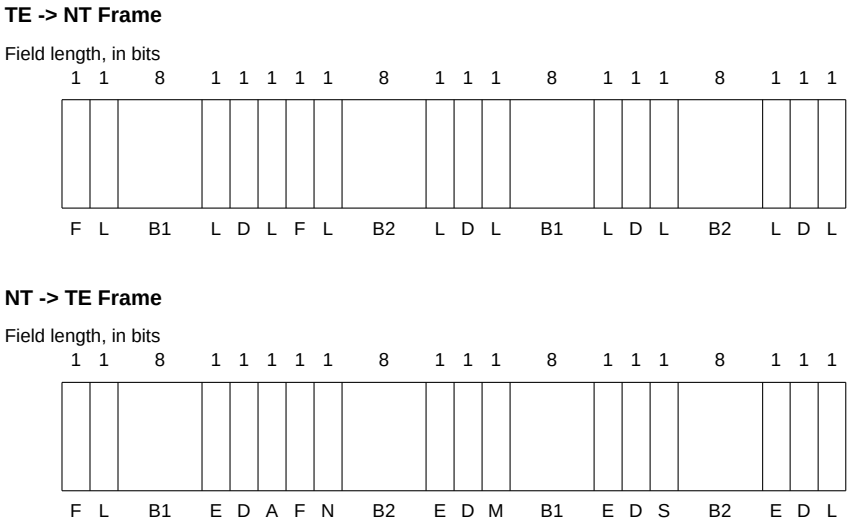
D-Channel Protocols In Depth

Layer 1

There are two principal Layer 1 protocols for ISDN BRI: ITU/CCITT Recommendation I.430 for TE to NT/NT to TE communication and ANSI T1.601 for NT to LE communication.

ISDN physical-layer (layer 1) frame formats differ depending on whether the frame is outbound (from terminal to network) or inbound (from network to terminal). Figure 13 shows the two I.430 frame formats.

Figure 13. 1.430 Frame Formats



The frames are 48 bits long, of which 36 bits represent data. The bits of an ISDN physical-layer frame are used as follows:

- F—Framing bit
- L—DC balancing bit
- D—D-channel bit
- E—Echo D-channel bit
- F—Auxiliary framing bit
- A—Activation bit
- N—Bit set to the complement of F
- B1—Bit within B-channel 1
- B2—Bit within B-channel 2
- S—Reserved for future standardization
- M—Multiframing bit

Four thousand frames are transmitted every second (each lasting 250 µs). For BRI, this yields a bit rate of 192 kbps. Each frame contains 16 bits from each of the two B channels and 4 bits from the D channel, yielding the data rates of 64 kbps and 16 kbps, respectively.

Multiple ISDN user devices can be physically attached to one circuit. In this configuration, collisions can result if two terminals transmit simultaneously. ISDN therefore provides features to determine link contention. When an NT receives a D bit from the TE, it echoes back the bit in the next E-bit position. The TE expects the next E bit to be the same as its last transmitted D bit. Terminals cannot transmit into the D channel unless they first detect a specific number of ones (indicating no signal) corresponding to a preestablished priority. If the TE detects a bit in the echo (E) channel that is different from its D bits, it must stop transmitting immediately. This simple technique ensures that only one terminal can transmit its D message at one time. After successful D message transmission, the terminal has its priority reduced by requiring it to detect more continuous ones before transmitting. Terminals cannot raise their priority until all other devices on the same line have had an opportunity to send a D message. Telephone connections have higher priority than all other services, and signaling information has a higher priority than nonsignaling information.

The ITU BRI specification describes the physical interface between the TE and the NT equipment. ITU standards do not address the physical connection across the local loop between the NT equipment (NT1) and the ISDN LE, or the U reference point. ANSI T1.601 addresses this part of the connection. While there are many differences between the I.430 and the T1.601 specs, the key differences revolve around the wiring, the line coding schemes, and the subsequent line speed. I.430 uses two pairs to communicate between TE and NT. T1.601, on the other hand, only uses one pair. This allows the standard two-wire pair (the local loop) that runs from the LE to the

customer premises to be used for ISDN. Additionally, while I.430 operates at 192 kbps, T1.601 operates at 160 kbps. This discrepancy is a result of different line coding schemes. I.430 employs a pseudo-ternary scheme, while T1.601 uses a 2B1Q scheme. In both cases, the user data rate remains at 144 kbps (two 64-kbps B channels, one 16-kbps D channel).

Table 5 shows a brief comparison of the I.430 and the T1.601 specs.

Table 5. Comparison of I.430 and T1.601 Specifications

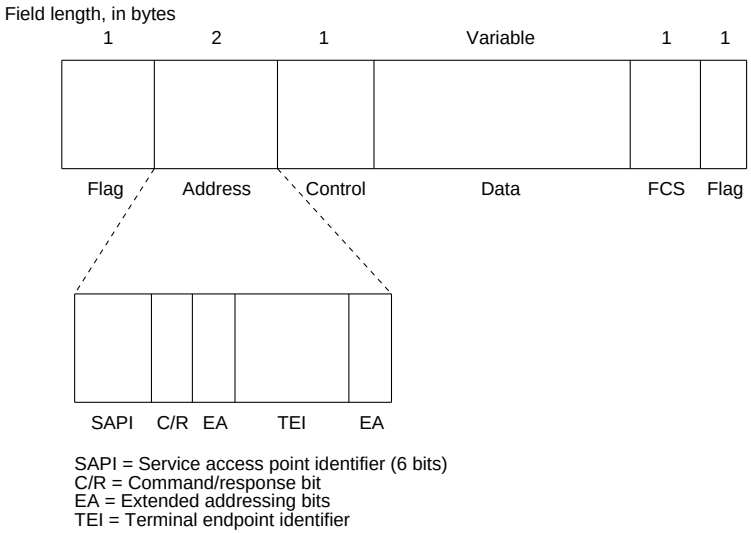
Specification	ITU I.430	ANSI T1.601
Reference Point	S or S/T	U
Devices	TE1/TA to NT	NT1 to LE
Physical configuration	Point to point	Point to point
	Point to multipoint	
	Serial	Serial
	Synchronous	Synchronous
	Full-duplex	Full-duplex
Bit rate	192 kbps	160 kbps
User date rate	144 kbps	144 kbps
Signaling scheme	Pseudo-ternary	2B1Q
Signaling baud	192 Kbaud	80 Kbaud
Timing source	NT	LE
No. of wiring pairs	2	1
No. of bits per frame	48	240
No. of bits user data	36	216
No. of bits overhead	12	24
No. of frames per sec.	4000	666.666…

Layer 2

Layer 2 of the ISDN signaling protocol is Link Access Procedure, D channel, also known as LAPD. LAPD is similar to HDLC and LAPB. As the expansion of the LAPD acronym indicates, it is used across the D channel to ensure that control and signaling information flows and is received properly. The LAPD frame format is very similar to that of HDLC and, like HDLC, LAPD uses supervisory, information, and unnumbered frames. The LAPD protocol is formally specified in ITU-T Q.920 and ITU-T Q.921. LAPD defines the logical connection on the D channel between the user (TE or TA) and the network (NT2 or LE) across the S (or S/T) reference point or between the user (NT2) and the network (LE) across the T reference point. It supports serial, synchronous, full-duplex transmission across either point-to-point or point-to-multipoint physical connections.

Figure 14 shows the LAPD frame format.

Figure 14. LAPD Frame Format

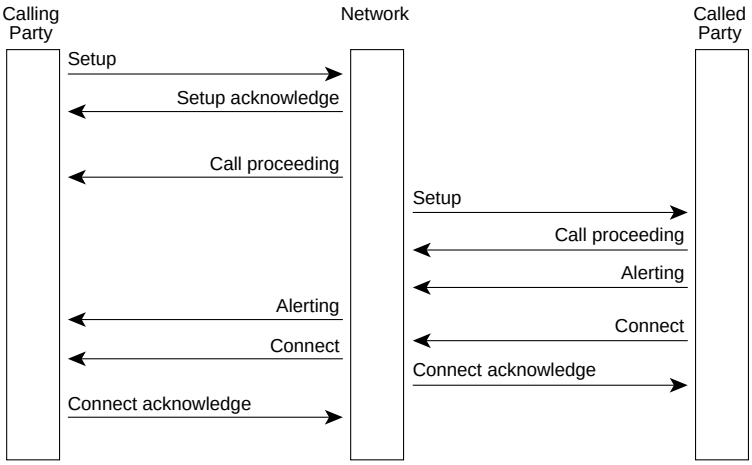


The LAPD flag and control fields are identical to those of HDLC. The LAPD address field can be either one or two bytes long. If the extended address bit of the first byte is set, the address is one byte; if it is not set, the address is two bytes. The first address field byte contains the service access point identifier (SAPI), which identifies the portal at which LAPD services are provided to layer 3. The C/R bit indicates whether the frame contains a command or a response. The terminal endpoint identifier (TEI) field identifies either a single terminal or multiple terminals. A TEI of all ones indicates a broadcast.

Layer 3

Two layer 3 specifications are used for ISDN signaling: ITU-T (formerly CCITT) I.450 (also known as ITU-T Q.930) and ITU-T I.451 (also known as ITU-T Q.931). Together, these protocols support user-to-user, circuit-switched, and packet-switched connections. A variety of call establishment, call termination, information, and miscellaneous messages are specified, including SETUP, CONNECT, RELEASE, USER INFORMATION, CANCEL, STATUS, and DISCONNECT. These messages are functionally similar to those provided by the X.25 protocol. Figure 15 shows the typical stages of an ISDN circuit-switched call.

Figure 15. ISDN Messages for Call Establishment



APPENDIX B: ISDN B-Channel Aggregation

As discussed earlier, a BRI has two separate 64-kbps B channels. In many cases, however, users want to aggregate both B channels to deliver 128 kbps of bandwidth. Presently there are two different aggregation solutions: static aggregation and dynamic aggregation. The following is a brief discussion of various aggregation techniques that fall under these two categories.

Static Aggregation Solutions

Static Dialing

Static dialing involves a router making a decision to initiate the dialing of a group of B channels simultaneously in the hope that the path across the ISDN network will be common. Load sharing would then be employed across B channels. This technique is no longer common, because it provides no control for the effective use of bandwidth.

Multirate ISDN Signaling

Multirate ISDN signaling requires the router to send a special call setup message to the local switch to identify the need for a call of predefined bandwidth. Such calls are more commonly referred to as H-channel calls. (See the H-channel discussion in Appendix A for bandwidth parameters.) H-channel calls are effective when the need for predefined bandwidth can be ascertained. Videoconferencing, which requires a fixed bit rate, would make good use of this technique. Dial-backup for leased line would also use this technique effectively. H-channel calls, however, are not effective where traffic flow is inconsistent because of the potential for wasted bandwidth. Note that not all ISDN switch types currently support signaling that allows H-channel calls.

Dynamic Bandwidth Aggregation

Dynamic Bandwidth Dialing

Dynamic bandwidth dialing normally relies on some form of load measurement on one or more B channels. The router then uses this loading factor in its decision-making process as to whether another B channel is required. Various proprietary algorithms can be employed by the router to share data across the B channels.

BONDING

BONDING has commonly been misused to describe any type of bandwidth aggregation. Actually, BONDING is an acronym for a very specific protocol: (**B**andwidth **ON D**emand **IN**teroperability **G**roup). BONDING is a protocol for circuit-switched aggregation of ISDN B channels to form a synchronous channel at the aggregate bit rate. With BONDING, the router places data within a framing structure that is then transmitted over multiple B channels. At the receiving end, the channels are phase-aligned and synchronized (using the framing structure) to recreate the original data stream. The framing and synchronization is process intensive and normally requires hardware assistance. Again, videoconferencing applications fare well with this technique.

PPP Multilink

PPP Multilink is the new IETF standard for B-channel aggregation (RFC 1717). PPP Multilink differs from BONDING in that it specifies B-channel aggregation at the packet level rather than at the bit level. Additionally, with PPP Multilink, the router does not specify how a router should accomplish the decision-making process for bringing up an extra B channel. Instead the router only ensures that packets arrive in sequence. To that end, data is encapsulated within PPP, and the datagram is given a sequence number. The receiving router uses the sequence number to recreate the original stream. PPP Multilink also provides the ability to segment data packets before encapsulation to improve resequencing/reassembly performance.

Cisco's Bandwidth Aggregation Strategy

As part of its ongoing commitment to ISDN development, Cisco will continue to deliver industry-standard solutions to customer problems. Presently all Cisco routers support dynamic bandwidth dialing using Cisco's bandwidth-on-demand (BOD) facility. This allows Cisco routers to initiate multiple B-channel calls on demand based on a user-defined load threshold. Refer to the "Bandwidth-on-Demand" section earlier in this document for specific configuration information.

Later in the 1995 calendar year, Cisco will introduce support for PPP Multilink. Additionally, as the use of H channels increases, Cisco will offer support for the necessary signaling. There are currently no plans to support BONDING.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Cisco Systems has over 100 sales offices worldwide. Call the company's corporate headquarters (California, USA) at 408 526-4000 to contact your local account representative or, in North America, call 800 553-NETS (6387).