Module 4: ISDN and DDR

Module Overview

4.1 ISDN Architecture
- 4.1.1 ISDN versus asynchronous dialup
- 4.1.2 ISDN services and channelized E1 and T1
- 4.1.3 BRI call processing
- 4.1.4 BRI functional groups and reference points
- 4.1.5 Physical representation of BRI reference points
- 4.1.6 PRI reference points

4.2 ISDN Protocol Layers
- 4.2.1 ISDN Layer 1
- 4.2.2 ISDN Layer 2 – Q.921
- 4.2.3 ISDN Layer 3 – Q.931
- 4.2.4 ISDN call setup
- 4.2.5 ISDN call teardown

4.3 Configuring ISDN BRI
- 4.3.1 ISDN BRI configuration overview
- 4.3.2 Configuring the ISDN switch type
- 4.3.3 Configuring the SPIIDs
- 4.3.4 Configuring the encapsulation protocol

4.4 Configuring Dial-on-Demand Routing (DDR)
- 4.4.1 DDR configuration overview
- 4.4.2 Defining interesting traffic
- 4.4.3 Assigning the dialer list to an interface
- 4.4.4 Defining destination parameters
- 4.4.5 Defining optional call parameters

4.5 Static and Default Routing
- 4.5.1 Use of static and default routes
- 4.5.2 Configuring static routes
- 4.5.3 Configuring default routes
- 4.5.4 Configuring route redistribution
- 4.5.5 Deactivating routing updates
- 4.5.6 Snapshot routing
- 4.5.7 Snapshot routing model
- 4.5.8 Enabling snapshot routing
- 4.5.9 Snapshot routing configuration example
Overview

This module introduces and describes a group of technologies called Integrated Services Digital Network (ISDN). When ISDN was proposed over thirty years ago, developers had recognized the natural limitations of the Plain Old Telephone Service (POTS). These developers envisioned that ISDN would provide a digital pipeline offering integrated access to the broadest range of services, such as voice, packet switching, and even video.

A number of ISDN standards were agreed upon over the years. These standards promised to bring high-speed digital service to homes and businesses. However, despite the extensive array of standards set for ISDN, carriers have not uniformly applied this technology. Consequently, ISDN configurations and pricing may vary significantly from region to region.

Today, customers use ISDN primarily as a WAN backup or to provide remote access to telecommuters and small offices. Service providers and large companies use Primary Rate Interface (PRI) to support large numbers of POTS, analog modem, and/or Basic Rate Interface (BRI) calls. Although ISDN has faster call setup and higher throughput than POTS, many potential BRI customers are turning to Digital Subscriber Line (DSL) and cable technologies. These technologies typically offer much higher throughput at a lower cost.

Despite these emerging technologies, ISDN remains a growing remote access solution for several reasons:

- ISDN is more widely available than DSL or cable.
- Many companies and service providers have made a significant investment in ISDN equipment and training and plan to continue supporting that investment.
- Remote offices using ISDN can connect to central offices without crossing the public Internet. Most DSL and cable implementations require the remote host to communicate with the central site using a VPN over the Internet.

This module covers ISDN technologies and describes how to configure ISDN using the Cisco IOS. This module also explores dial-on-demand routing (DDR), which is often used in ISDN configurations.

4.1.1 ISDN versus asynchronous dialup

Public Switched Telephone Network (PSTN) has many limitations, including:

- The PSTN is an analog network.
- The PSTN was originally designed for voice only communications, which limits its capabilities when using it for data communications.
- Computers must convert digital signals to analog and then back to digital in order to communicate over the PSTN.
- The analog local loop uses Pulse Code Modulation (PCM) to encode the analog signals for digital transmission. This type of analog-to-digital conversion introduces undesired latency and can introduce noise.
- The maximum transfer rate for an analog connection on the PSTN is 53 kbps.
- The PSTN operates at half-duplex only, which means it can send or receive data, but not both at the same time.
- Analog modems require significant time to establish a connection.
ISDN was developed to overcome the limitations of the PSTN:

- ISDN is an end-to-end digital network.
- ISDN allows digital services for data, voice, and video.
- It is available in bundles of 64 kbps.
- ISDN operates in full-duplex mode. In full-duplex mode, data can be transmitted and received simultaneously.
- ISDN has quick call setup.

The following sections describe the two different ISDN services available to customers. These two services are BRI and PRI.

### 4.1.2 ISDN services and channelized E1 and T1

ISDN is available in two levels of service. Basic Rate Interface (BRI) is intended for the home and small enterprise. Primary Rate Interface (PRI) is intended for larger users, such as ISPs and corporations. Both services include B channels and a D channel.

B channels are called bearer channels because they carry voice, data, and fax transmissions. The B Channel Layer 2 frame format is High-Level Data Link Control (HDLC) or Point-to-Point Protocol (PPP).

The D channel, or delta channel, is used for out-of-band signaling. The D Channel carries control messages, such as call setup and teardown. Typically, the D channel employs Link Access Protocol D (LAPD) at Layer 2.

BRI service is provided over a local copper loop that traditionally carried analog phone service. The maximum length of most ISDN local loops in North America is approximately 5.5 kilometers (18,000 feet or 3.41 miles).

BRI has the following characteristics:

- Two 64-kbps bearer channels
- One 16-kbps delta channel
- 48 kbps of framing and synchronization information
- Total speed of 192 kbps

It is important to know which of the BRI characteristics is being referenced when discussing ISDN BRI bandwidth. If referencing the bandwidth available for user data, ISDN BRI provides 128 kbps, which is two 64-kbps B channels. If referencing the bandwidth of both B channels and the D channel, ISDN BRI provides 144 kbps. 144 kbps is two 64-kbps B channels plus one 16 kbps D channel. Although not commonly done, if referencing ISDN BRI, including framing and synchronization, the total bandwidth is 192 kbps. 192 kbps is two 64-kbps B channels plus one 16 kbps D channel plus 48 kbps for framing and synchronization.

ISDN PRI service is provided over T1 and E1 leased lines between the customer premise equipment (CPE) and the ISDN switch. A T1 is made up of twenty-four Digital Signaling Zero (DS0) channels.

PRI over T1 specifies the following:

- Twenty three 64-kbps bearer channels
- One 64-kbps D channel, carried in timeslot 24
8 kbps of framing and synchronization information
Total speed of 1.544 Mbps

PRI over E1 provides the following:

- Thirty 64-kbps bearer channels
- One 64-kbps D channel, carried in timeslot 16
- 64 kbps of framing and synchronization information
- Total speed of 2.048 Mbps

4.1.3 BRI call processing

When a BRI call is initiated, the CPE sends the called number to the local ISDN switch using the D channel.

The local switch uses the Signaling System 7 (SS7) protocols to set up a path inside the public switched telephone network (PSTN). The number that was called is passed to the terminating ISDN switch. This remote switch brings up the D channel to the destination. Remember that the D channel is used for the call-control functions. These functions include call setup, signaling, and call termination. ISDN is a local-loop technology. After the ISDN switch processes the call, SS7 is used to transport data of the carrier.

When the terminating CPE answers, the B channel is connected end to end. The B channel carries the conversation or data. Both B channels can be used simultaneously to connect to the same destination or to different destinations.
4.1.4 BRI functional groups and reference points

ISDN is a distinct set of technologies. The International Telecommunications Union Telecommunication Standardization Sector (ITU-T) groups and organizes the ISDN protocols according to general topics.

It is not necessary to know all the rules. However, it is important to be familiar with the E, I, and Q designations and with the general topics that each represents.

In addition to defining protocols, ISDN standards specify the function of a given device in the network. BRI can involve many functional devices, also known as functional groups. The following functional groups are also illustrated in Figure 2:

- **Terminal equipment 1 (TE1)** – Designates a device that is compatible with the ISDN network. Examples of TE1 include a digital telephone, a router with an ISDN interface, or digital facsimile equipment.
- **Terminal equipment 2 (TE2)** – Designates a device that is not compatible with ISDN. A TE2 device requires a terminal adapter. For example, a router without an ISDN interface is a TE2 device.
- **Terminal adapter (TA)** – Connects non-ISDN devices to an ISDN network. A TA converts standard electrical signals into the form used by ISDN. For example, a TA converts V.35 or EIA/TIA-232 to ISDN. Essentially, it is an ISDN modem.
- **Network termination type 1 (NT1)** – Connects four-wire ISDN subscriber wiring to the conventional two-wire local-loop facility. NT1 inside the CPE is used in North America, whereas ISDN S/T interfaces are used throughout most of the world.
- **Network termination type 2 (NT2)** – Directs traffic to and from different subscriber devices and the NT1. The NT2 is an intelligent device that performs switching and concentrating. A private branch exchange (PBX) is often the NT2 device.
- **Line termination (LT)** – This is the part of the telco that interfaces with the CPE. In Europe it functions as a termination for the U interface.
- **Exchange termination (ET)** – This point is where the subscriber line cards are used in the ISDN exchange. It is where the Layer 2 information (for example LAPD) will be terminated in the ISDN Exchange.
- **Local Exchange (LE)** – LE is the point where the ISDN switch is housed in the central office (CO). The LE implements the ISDN protocol and is part of the
Two types of data terminal equipment (DTE), TE1s and TE2s, can use ISDN services.

BRI requires an NT1 in order to connect to an ISDN switch on the carrier. Some devices, such as routers, combine both TE1 and NT1 functionality in the same unit.

The ISDN reference points define how the functional groups, such as TE2 and TA, connect to each other. The ISDN reference points are as follows:

- **User reference point (U)** – The user reference point is located between the NT1 and LT. The U interface corresponds with a subscriber line. There are no ITU-T standards for the U interface. This is the American National Standards Institute (ANSI) standard for the United States.

- **Terminal reference point (T)** – Located between the NT1 and NT2 or between the NT1 and TE1 or TA, if there is no NT2 device. In BRI, the T interface uses the same characteristics as the S interface. Therefore, the two reference points are typically combined in a single interface, referenced as an S/T interface.

- **System reference point (S)** – Located between the NT2 and TE1 or TA. The S interface connects the terminals to the ISDN network. This interface is the most important for users. The S interface uses the same characteristics as the T interface.

- **Rate reference point (R)** – Located between TA and TE2. TE2 is a non-ISDN interface. The TE2 connects to the TA using a standard physical-layer interface. These standards include EIA/TIA-232-C, V.24, X.21, and V.35. EIA/TIA-232-C was formerly RS-232-C.

Reference points are architectural definitions that may or may not physically exist as separate elements in a network. For example, some routers have one or more U interfaces. This means those routers can connect directly to the ISDN switch of a carrier. In this type of network, the S, T, and R reference points would not exist. Some manufacturers define a V reference point in LEs between LT and ET. This reference point identifies the network node interface and is transparent to users.
The numerous ISDN abbreviations and acronyms may be confusing. However, it is important to have a good knowledge of these components and reference points when setting up and troubleshooting ISDN.

In Figure 1, a connection is made from the wall jack with a standard two-wire cable to the NT1. From the NT1, a four-wire connection is made to an ISDN phone, Cisco ISDN router, and a terminal adapter that is attached to a non-ISDN fax. The S/T interface is commonly identified as a four-wire interface but is actually implemented using an eight-wire connector. The four-wire interface is only referring to the transmit and receive lines. Two wires are transmit lines and the other two wires are the receive lines. Of the remaining four wires, two are power lines used for powering the NT and TE. The remaining two wires are unused.

The S/T interface defines the interface between a TE1 or TA and an NT. The S/T reference point is an interface composed of two twisted pairs, one for TX, the other for RX. It uses the ITU I.430 specification.

The U interface defines the two-wire interface between the NT and the ISDN cloud. The R interface defines the interface between the TA and an attached non-ISDN device (TE2).

An NT1 and NT2 combination device is sometimes referred to as a Network Termination.
A regular ISDN S interface can have several endpoint devices with different capabilities occupying the same bus, the "S" bus. When the switch can communicate with multiple devices, it is typically referred to as "multipoint". Unfortunately, this creates complexity in both ISDN device setup and call processing. This complexity requires the use of service profile identifiers (SPIDs) and endpoint identifiers (EIDs).

When selecting ISDN equipment, it is important to know the reference point that defines the type of ISDN interface needed. In North America, a U interface is typically required to connect to a provider. This means if an ISDN router with an S/T interface is purchased, an additional NT1 device will be required to connect to the provider’s network. Connecting a S/T BRI router interface to a U telco outlet by mistake can cause permanent damage to the device. Therefore, it is important to know the ISDN reference points to properly select and install ISDN devices.

Figure 2 shows a Cisco 1003 router with an S/T interface connected to an NT1. The NT1 connects to an ISDN switch, owned by the provider, using a local loop. An ISDN switch typically resides at the provider’s site. However, in Figure 3, the Adtran Atlas 550 WAN emulation device is used to emulate the ISDN switch.

Figure 3 displays a Cisco 2620 with a U-interface directly connected to the ISDN switch (Atlas 550) using the local loop.

4.1.6 PRI reference points
ISDN PRI is delivered using a leased T1 or E1 line. A channel service unit/data service unit (CSU/DSU) is required to connect a router, the TE, and to the carrier network. Internal CSU/DSUs are common among modular routers.

The PRI reference points are more straightforward than BRI reference points. The PRI reference points can contain numerous functional groups in a multipoint configuration.

Why not just get a leased line in the first place? ISDN PRI does require a leased line and offers the same total bandwidth as a leased line. In fact, the primary application for ISDN PRI is modem aggregation, not high-capacity point-to-point connectivity.

If the throughput of a DS1, 1.544 Mbps, is needed, then a dedicated line is the
appropriate solution. PRI offers a powerful solution for a service provider or a large company that supports dozens of dialup remote access connections.

The term DS1 stands for digital service 1. DS1 is an interface with a 1.544 Mbps data rate that often carries voice connections on a PBX. Each DS1, also known as T1, has 24 DS0 channels framed together so that each DS0 timeslot can be assigned to a different type of trunk group, if desired.

ISDN PRI supports hybrid dialup access using a single phone number. One PRI over T1 can support up to 23 dialin calls. These calls can be either analog POTS calls or digital ISDN BRI calls. The callers dial the same phone number although they are each connected to a different channel. PRI makes analog calls at 53.3 kbps, using 56K modems. This is possible because each channel is a DS0, 64 kbps. The D channel identifies if the call is a circuit-switched digital call or an analog modem call. Routers can be configured to decode analog modem calls and then send them to the onboard modems. Circuit-switched digital calls are directly relayed to the ISDN processor in the router.

In a typical configuration, an access server, such as a Cisco 3660, contains an integrated digital modem and a channelized T1 controller. The T1 controller connects to a leased T1 line, which provides connectivity to the ISDN cloud. This setup allows ISDN routers and analog modems to connect to the access server simultaneously.

4.2.1 ISDN Layer 1

ISDN at Layer 1 is responsible for switching the carriers circuits to build a connection. ISDN Layer 1 also supports the attachment of various ISDN functional devices. Both the B and the D channels share this physical layer. Layer 1 ISDN standards include the following:

- I.430 for BRI, which defines the communication across the S/T reference point
- I.431 for PRI, which is a full-duplex, point-to-point, serial, synchronous connection
- ANSI T1.601 for BRI, which defines the communication across the U interface for North America

<table>
<thead>
<tr>
<th>Layer 3</th>
<th>Layer 2</th>
<th>Layer 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>D Channel</td>
<td>B Channel</td>
<td>D Channel</td>
</tr>
<tr>
<td>DSS1 (Q.931)</td>
<td>IP/IX</td>
<td>I.430/I.431/ANSI T1.601</td>
</tr>
<tr>
<td>LAPD (Q.921)</td>
<td>HDLC/PPP/FR/LAPB</td>
<td></td>
</tr>
</tbody>
</table>

4.2.2 ISDN Layer 2 – Q.921

The ISDN D and B channels use different protocols at Layers 2 and 3. The B channel typically frames data using either PPP or HDLC. ISDN is most commonly
configured to use PPP. This is because PPP can support additional features, such as authentication and bandwidth aggregation.

As specified by Q.921, the D channel typically frames data using LAPD. LAPD is a version of Link Access Procedure, Balanced (LAPB) modified for the ISDN D channel. At Layer 3, the D channel uses the Q.931 protocol, which is part of the Digital Subscriber Signaling System No. 1 (DSS1) suite of protocols. DSS1 is a set of Layer 3 protocols that establish the connection between a device and the ISDN network. A simple way to distinguish between these protocols is to associate the “2” in Q.921 with Layer 2 and the “3” in Q.931 with Layer 3.

With ISDN, all hardware addressing occurs in Layer 2, just like in a traditional LAN environment. It is possible to have up to eight ISDN terminals on an S/T bus. In order for ISDN to tell the difference between TEs, each TE must have a unique address. One part of the ISDN Layer 2 address is called a terminal endpoint identifier (TEI).

The TEI is a 7-bit number carried in the address field of the LAPD frame on the D channel. Typically, the TEI is dynamically assigned to a TE, such as an ISDN router, by the ISDN switch. The ISDN switch assigns a TEI upon receiving a request from the TE. Generally, the TE makes this request when it first powers up. There are three ranges of TEI addresses as follows:

- 0-63 for non-automatic TEI assignment
- 64-126 for automatic TEI assignment
- 127 for group assignment, or broadcast

The TEI works together with the service access point identifier (SAPI) to complete the Layer 2 address. The SAPI is a 6-bit number used to identify and manage different data types for the same individual device connecting to the ISDN network. Remember, some ISDN messages are for call setup or teardown while others are actual data. Therefore, the TEI represents the specific ISDN device while the SAPI represents the specific process running on that device. For example, the SAPI value 0 is used to identify call-control procedures, while the SAPI value 63 identifies a Layer 2 management function.

Just as an Ethernet II frame contains the destination MAC address and the protocol type information, the LAPD frame contains a TEI and a SAPI value.
4.2.3 ISDN Layer 3 – Q.931

At Layer 3, the B channel can carry datagrams using a variety of Layer 3 protocols, including IP, IPX, and AppleTalk. The D-channel uses the Q.931 at Layer 3. Q.931 is used to communicate between an ISDN switch of a carrier and a customer TE device such as a router. In BRI, this protocol is transparent to the NT1 device.

When configuring a router for an ISDN connection, the type of ISDN switch being used must be specified. The switch must be specified because different ISDN switches use different Q.931 messaging procedures. If the incorrect switch is specified, D channel communication will not occur. When an ISDN service is requested, the provider will furnish the ISDN switch information.

4.2.4 ISDN call setup

An ISDN call can be placed in numerous ways. In an ISDN call, the calling party requests...
Several progress messages may be displayed before the actual connect and call proceeding. These optional messages indicate how the call is proceeding.

For example, the alerting message is an optional message. It is typical of telephone messages, but is not required. Alerting messages are not typical with data transmissions. Most of the time, connection messages are seen with data calls.

Different ISDN switches use different call setup and teardown procedures. Therefore, not all the steps shown in the figure may be executed. At a minimum, setup, call proceeding, connect, and connect acknowledge messages should be exchanged.

4.2.5 ISDN call teardown

The call teardown request is not an end-to-end function but instead is processed by the ISDN switch. This process is similar to call setup. The release procedures are based on a three-message approach as shown:

- Disconnect
- Release
- Release complete

The release message is transmitted through the network as quickly as possible. Figure 1 assumes that the called party is generating the release. The process is initiated by a disconnect message on the D channel, between the calling and called parties. After receiving this disconnect message, the exchange immediately starts the release of the switch path that supports the B-channel circuit. A release message is also sent to the succeeding exchange at the same time. The message is passed through the network from all intermediate exchanges to the terminating exchange.

As the involved exchanges release the call, a released message is eventually transmitted to the terminating exchange. This transmission causes the following actions:

- The transmission issues a disconnect message to the calling party.
• It starts a timer to ensure receipt of a released message.
• It disconnects the switched path.
• When a released message is received from the preceding exchange, it returns a release complete message to the preceding exchange.

4.3.1 ISDN BRI configuration overview

Global and interface configuration commands are required to configure ISDN on a Cisco router. This section focuses on configuring BRI for access routers.

In global configuration mode, the ISDN switch of the service provider must be configured. There are several types of switches to choose from. The choice of switch type varies according to its geographical location. Some of the switches require special parameters. For example, the three most common types of switches in North America are the DMS-100, National-1, and AT&T 5ESS. The DMS and National switches require a special parameter called the service profile identifier (SPID) to be specified. SPIDs are optional on some switches. The AT&T 5ESS switch type may support SPIDs but it is recommended that the ISDN service be set up without them.

SPIDs have significance at the local access ISDN interface only. Remote routers are never sent the SPID.

ISDN interface addressing tasks include assigning the IP address, identifying the dialer group for DDR, ISDN service profile statements, and possible SPID numbers. A `dialer map` command may also be configured to associate a statically mapped destination to a destination IP address, hostname, and ISDN dial number.
### 4.3.2 Configuring the ISDN switch type

Different ISDN providers use different switch types. Some providers use software on one type of switch to emulate another type of switch. The ISDN carrier will provide the appropriate switch type information. If the router is not configured with the correct switch type information, it will not be able to communicate with the ISDN switch using Q.931 at Layer 3. Therefore, no ISDN call can be dialed or received.

Use the `isdn switch-type` command to configure the ISDN switch type being used. This command can be entered in either global or interface configuration mode.

The global `isdn switch-type` command sets all ISDN interfaces on the router to be configured for the same switch type:

```
Router(config)#isdn switch-type type
```

When issuing the `isdn switch-type` command in interface configuration mode, only the interface that is being configured assumes the switch type:

```
Router(config-if)#isdn switch-type type
```

Note that the interface configuration command overrides the global-level command.

Typically, the switch type is specified in global configuration mode using the `isdn switch-type` command. However, in some cases, two different ISDN switch types might have to be configured. An example would be when the same router connects to both BRI and PRI. For this reason, Cisco extended the use of the command to the interface configuration mode beginning with IOS release 11.3.

The `interface bri interface-number` command designates an ISDN interface on a router that natively supports ISDN (TE1). Therefore, enter the following to configure the

---

**ISDN Configuring Tasks**

- **Global Configuration**
  - Select switch type
  - Specify traffic to trigger DDR call

- **Interface Configuration**
  - Select interface specifications
  - Configure ISDN addressing

- **Optional feature configuration**
first ISDN interface with the AT&T basic rate switch type:

```
RTA(config)#interface bri 0
RTA(config-if)#isdn switch-type basic-5ess
```

If the router is a TE2 device, which does not have a native BRI, it must use an external ISDN terminal adapter. On a TE2 router, configure the appropriate serial interface to send the ISDN traffic to the TA.

For BRI ISDN service, the switch type can be one of several. Different switch types will vary, depending on the version of Cisco IOS software used.

<table>
<thead>
<tr>
<th>Switch Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>basic-5ess</td>
<td>AT&amp;T basic rate switches (United States)</td>
</tr>
<tr>
<td>basic-dms100</td>
<td>NT DMS-100 (North America)</td>
</tr>
<tr>
<td>basic-ni</td>
<td>National ISDN (North America)</td>
</tr>
<tr>
<td>basic-1t6</td>
<td>German T1R5 ISDN switches</td>
</tr>
<tr>
<td>basic-norwe3</td>
<td>Norwegian Net3 switches</td>
</tr>
<tr>
<td>basic-nznet3</td>
<td>New Zealand Net3 switches</td>
</tr>
<tr>
<td>basic-austr3</td>
<td>Australian T013 and T014</td>
</tr>
<tr>
<td>basic-net3</td>
<td>Switch type for NET3 in United Kingdom and Europe</td>
</tr>
<tr>
<td>ntt</td>
<td>NTT ISDN switch (Japan)</td>
</tr>
</tbody>
</table>

### 4.3.3 Configuring the SPIIDs

A service profile identifier (SPID) is a number provided by the ISDN carrier to identify the line configuration of the BRI service. SPIIDs allow multiple ISDN devices, such as voice and data, to share the local loop. DMS-100 and National ISDN-1 switches require SPIIDs. Depending on the software on an AT&T 5ESS switch, SPIIDs may be required.

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

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

DMS-100 and National ISDN-1 switches support only two SPIIDs per BRI. One SPIID is supported for each B channel. If both B channels will be used for data only, configure the router for both SPIIDs, one for each B channel. Data and voice cannot run over the same B channel simultaneously. The absence or presence of a channel SPID in the configuration of the router dictates whether the second B channel can be used for data or voice.

To keep SPID numbers simple, most telephone companies use part of the ISDN phone number in the SPID naming system. Therefore, SPIIDs are often the ISDN phone number with some optional numbers. For example, the SPID for the phone number 888-555-1212 could be 888555121200.

A local directory number (LDN) might also be necessary if the router is to answer calls made to the second directory number. The commands to set SPIIDs and LDNs on both B
channels are as follows:

```
Router(config-if)#isdn spid1 spid-number [ldn]
Router(config-if)#isdn spid2 spid-number [ldn]
```

The service provider will supply the necessary SPID configuration information.

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>isdn spid1 and isdn spid2</td>
<td>These commands are used to define, at the router, the service profile identifier (SPID) number that has been assigned by the ISDN service provider for the respective B channel.</td>
</tr>
<tr>
<td>spid-number</td>
<td>This is the number that identifies the service to which you have subscribed. The ISDN service provider assigns this value.</td>
</tr>
<tr>
<td>ldn</td>
<td>This local dial number (optional) must match the called-party information coming in from the ISDN switch in order to use both B channels on most switches. This is a seven digit number that will be assigned by the ISDN service provider if required.</td>
</tr>
</tbody>
</table>

### 4.3.4 Configuring the encapsulation protocol

A method of datagram encapsulation is needed for data to be transported when dial-on-demand routing (DDR) or a user creates an end-to-end path over ISDN. Available encapsulations for ISDN include the following:

- PPP
- HDLC
- Frame Relay
- LAPB
- Combinet Proprietary Protocol (CPP)

LAPB can also be used for datagram delivery over the D channel.

The most common Layer 2 encapsulation protocol is PPP. Dynamic Multiple Encapsulations feature (introduced in Cisco IOS Release 12.1) allows incoming calls over ISDN to be assigned an encapsulation type such as Frame Relay, PPP, and X.25 based on Calling Line ID (CLID) or Dialed Number Identification Service (DNIS). Enter the following command to configure encapsulation for the ISDN interface:

```
Router(config-if)#encapsulation [ppp | lapb | hdlc | x25 | cpp]
```

Use the `encapsulation hdlc` command to revert from PPP encapsulation to the default encapsulation.

If the ISDN interface will receive calls from more than one dialup source and PPP encapsulation is configured, authentication should also be configured. Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) are two PPP authentication features. The following example represents a typical BRI encapsulation configuration using PPP with CHAP:

```
Router(config)#interface bri 0
Router(config-if)#encapsulation ppp
Router(config-if)#ppp authentication chap
```

Several other important configuration commands can be used with BRI. These other
4.4.1 DDR configuration overview

With dial-on-demand routing (DDR), connections initiated by remote offices or telecommuters are only activated as needed. This will result in substantial cost savings for the company. In DDR scenarios, routers are not connected for long periods of time. Because ISDN provides greater throughput and quicker call setup than POTS, DDR is most often used with ISDN.

The four basic steps to DDR configuration are as follows:

1. Define what constitutes interesting traffic by using the **dialer-list** command.
2. Assign this traffic definition to an interface by using the **dialer-group** command.
3. Define the destination address, hostname, and telephone number to dial by using the **dialer map** command.
4. Define call parameters by using other dialer commands, such as **dialer idle-timeout**, **dialer fast-idle**, and **dialer load-threshold** (Optional).
4.4.2 Defining interesting traffic

The `dialer-list` command is used to define what type of traffic is "interesting". A router will bring up a DDR interface, if it is not up already, to route interesting traffic. Once the call is established, the router will not disconnect the call as long as it continues to receive interesting traffic to route over the DDR link. While the link is up, other "uninteresting" traffic can be routed over the link. Uninteresting traffic is traffic that is not defined by the dialer list. However, if the link is idle for a configurable period of time, the router will disconnect the call. The router considers the link idle if it is not being used to route interesting traffic. Every time interesting traffic is routed out a DDR interface, the idle timer is reset. Therefore, traffic that is uninteresting will not keep a DDR call established.
The simple form of the `dialer-list` command specifies whether a whole protocol suite, such as IP or IPX, will be permitted to trigger a call. The more complex form of the `dialer-list` command references an access list. This allows finer control of the definition of interesting traffic.

Configure a simple dialer list using the following syntax:

```
Router(config)#dialer-list dialer-group-number
protocol protocol-name {permit | deny}
```

The following example configures a dialer-list that will trigger a call for any IP traffic:

```
RTA(config)#dialer-list 1 protocol ip permit
```

The `access-list` command specifies interesting traffic that initiates a DDR call. The `dialer-list` command is used with the access list:

```
Router(config)#access-list access-list-number [permit | deny] {protocol | protocol-keyword} {source source-wildcard | any} {destination destination-wildcard | any} [protocol-specific-options] [log]
Router(config)#dialer-list dialer-group list access-list-number
```

The following example configures an access list and a dialer list so that only traffic from one host is considered interesting:

```
Router(config)#access-list 24 permit host 192.168.1.2
Router(config)#dialer-list 1 list 24
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dialer-list</code></td>
<td>This command defines a DDR dialer list to control dialing by protocol, or by a combination of protocol and a previously defined access list.</td>
</tr>
<tr>
<td><code>protocol protocol-name</code></td>
<td>This is the number of a dialer access group identified in any dialer group interface configuration command.</td>
</tr>
<tr>
<td>`deny</td>
<td>list access-list-number`</td>
</tr>
<tr>
<td><code>access-list-number</code></td>
<td>This is the number of the access list to be referenced.</td>
</tr>
</tbody>
</table>

### 4.4.3 Assigning the dialer list to an interface

Once the dialer list is created, it needs to be assigned to any interface responsible for initiating the call. This is accomplished by using the `dialer-group` command. The dialer group is referenced in the `dialer-list` command:

```
Router(config)#dialer-list 1 protocol ip permit
Router(config)#interface bri 0/0
```
Router(config-if)#\texttt{dialer-group 1}

\textbf{Note:} Only one access list can be specified in the \texttt{dialer-list} command for any given protocol and any given dialer group.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\texttt{dialer-group}</td>
<td>This command configures an interface to belong to a specific dialing group. The dialer group points to a dialer list.</td>
</tr>
<tr>
<td>\texttt{group-number}</td>
<td>This is the number of the dialer access group to which the specific interface belongs. This access group is defined with the \texttt{dialer-list} command, which specifies interesting traffic that initiates a DDR call. Acceptable values are nonzero, positive integers from 1 to 10.</td>
</tr>
</tbody>
</table>

### 4.4.4 Defining destination parameters

Once interesting traffic has been defined, the interface responsible for initiating the call with all the parameters necessary to reach the destination must be identified. The \texttt{dialer map} command identifies destination router information, such as the phone number to dial:

Router(config-if)#\texttt{dialer map protocol next-hop-address [name hostname] [broadcast] dial-string}

There are many other optional parameters available to the \texttt{dialer map} command. However, using the options displayed in the figure will suffice for most connections.

Cisco IOS commands often contain the word "map". This word is used in the command to statically map Layer 2 addresses to Layer 3 addresses. For example, the command \texttt{frame-relay map} is used to define a Layer 3 next-hop-address to its Layer 2 address, PVC number. With a \texttt{dialer-map} statement, a Layer 3 address, IP in this module, is linked to a dialup Layer 2 address. In this case, the dialup Layer 2 address is a phone number.

When setting up DDR between more than two sites, it is very important to use PPP authentication. Also, be sure to use the \texttt{name} keyword with the \texttt{dialer-map} command. Dialer maps for inbound calls are maps between protocol addresses and authenticated user names.
4.4.5 Defining optional call parameters

The following additional call parameters can be added to the interface:

```
Router(config-if)#dialer idle-timeout seconds
Router(config-if)#dialer fast-idle seconds
Router(config-if)#dialer load-threshold load [outbound | inbound | either]
```

Dialup connections are subject to an idle timer. The idle timer keeps track of how much time has elapsed since interesting traffic was routed out the interface. By default, the idle-timeout is set to 120 seconds. This value can be customized to make the timer more aggressive, or the timeout value can be increased to keep the connection up longer. To manually set the idle timeout value, use the `dialer idle-timeout` command.

When the router is waiting to use a line to make another call, it uses a more aggressive idle timeout called fast-idle. The fast-idle time is the number of seconds that a line can remain idle before the current call is disconnected to allow another call that is waiting to use the line. The `dialer fast-idle` command can be used to alter this value. The default value is 20 seconds.

The following commands configure short timeout periods, which may be appropriate for expensive toll lines:

```
RTA(config-if)#dialer idle-timeout 60
RTA(config-if)#dialer fast-idle 15
```

The `dialer load threshold` command is used to specify the interface load at which the router will initiate another call to the destination. This command is typically used with Multi-link PPP (MLP) ISDN connections and is explored later in this module.
4.5.1 Use of static and default routes

It may seem that DDR is only used to activate WAN links for the exchange of user data. However, dial-on-demand routing is also used to exchange routing information over intermittent links.

Routers make path determinations based on the information they have in their routing tables. Routing tables are built from dynamically learned routes and administratively defined routes, the static routes.

Dynamic routing can be a source of problems when used in a DDR environment. Most routing protocols rely on regular communication between link partners to exchange tables or keepalives. The problem is how to keep the routers converged while keeping WAN link costs down.

A common WAN solution is to control route advertisement with static and default routes. Default routes are typically configured on stub networks while static routes are configured on central site routers. Route redistribution may be necessary to share routing information between the different protocols.

Ultimately, static and default routing may be used to address the challenge of routing in a DDR network. However, dynamic routing and route redistribution may be required to propagate routes in complex networks. Simple distance-vector routing protocols, RIP and IGRP, are typically used over simple DDR connections. Fast-converging routing protocols, EIGRP, ISIS, and OSPF, are likely to operate over the WAN core of an enterprise.

Routing updates may need to be eliminated or controlled for use over intermittent WAN links. This can be accomplished in a variety of ways including passive-interfaces and snapshot routing. Each of these techniques is discussed in this module.

4.5.2 Configuring static routes

Static routes are entered manually. This eliminates the need for a routing protocol to send routing updates across the DDR connection. Static routes can be effective in small networks that do not change often.
Figure 1 displays a remote access scenario. This scenario has the central site configured with a static route to a network address or addresses of a remote site. Since the remote site is generally a stub network, its router is configured with a default route. This route points back to the central site router and the corporate network, which is represented by the cloud.

At the central site, there is a static route pointing towards an interface (the next hop) at the remote site SOHO:

```plaintext
Central(config)#ip route 172.24.2.0 255.255.255.0 10.2.3.2
```

A DDR router configured with this static route receives an interesting packet destined for the 172.24.2.0 /24 network. This router would refer to a dialer map statement that maps a phone number to the next hop IP address, 10.2.3.2.

It is possible to use one route to define the next-hop IP address. A second route can be used to define the interface on which to find the next-hop and dialer map. Therefore, a static route can be configured using the local interface from which traffic must exit to reach the destination network.

At least one static route pointing to the next-hop IP address is necessary for DDR to work. In Figure 4, the BR0/0 interface of RTA has three different dialer maps to three different remote routers. What will happen when RTA attempts to route traffic to 192.168.1.0 /24 out BR0/0? The router will not be able to determine the appropriate dialer map statement to be able to reach the destination network. This is because no next-hop address is specified in the static route. Even if RTA had only one dialer map statement configured on BR0/0, the router would still fail to route the packet.

Under most circumstances, the `ip route` command contains the IP address of the next hop. However, for routes over unnumbered point-to-point interfaces, the interface used to reach the destination should be specified.
Setting Default/Static Routes

Static route is toward the remote site

Default route is toward cloud

Configuring Static Routes

Central (config) # ip route 172.24.2.0 255.255.255.0 10.2.3.2
4.5.3 Configuring default routes

A stub network has only one path to the outside world. For this reason, a default route is normally the only route required on a remote network. Most remote offices are stub networks and are often configured with a default route.

To configure a static default route, use the `ip route` command as follows:

```
Router(config)#ip route 0.0.0.0 0.0.0.0 {next-hop-address | exit-interface}
```

On an IGRP router, the `ip default-network` command must be used so that the router will include the default route in its updates. IGRP does not understand a route to 0.0.0.0/0. The `ip default-network` command can be used with other routing protocols as well. For more information on the difference between the `ip route 0.0.0.0 0.0.0.0` command and the `ip default-network` command, refer to the Cisco Networking Academy Program: CCNP-1 course.

The figure displays the commands needed to configure a default route on the SOHO router. Once configured with this default route and dialer map, the SOHO router will route all non-local traffic over the dialup link.
4.5.4 Configuring route redistribution

When static routes are used on the central site router, they typically need to be redistributed into a dynamic routing protocol. This redistribution allows other routers in the enterprise to learn about the remote LAN dynamically. The router configuration mode `redistribute static` command can be configured to redistribute static routes.

The corporate network shown in the figure uses EIGRP as its backbone routing protocol. The Central router is configured to redistribute the static route to the SOHO LAN (172.24.2.0 /24) into EIGRP.

Dynamic routing can also be used in DDR networks in a number of ways. Dynamic routing can be used with snapshot routing. Snapshot routing is described later in this module. This will cache routes learned by dynamic routing protocols, thereby allowing the automation of static routing maintenance. Dynamic routing can also be used as a trigger for routing convergence in large and complex DDR designs.

When the DDR link is connected, routing updates will flow to the peer, allowing redundant designs to converge on the physical connection by redistribution of trigger routing updates.

The routing protocol selected for a DDR link is typically a distance-vector protocol such as RIP, RIPv2, EIGRP, IGRP, or RTMP. OSPF can be used if configured with the On-Demand Circuit feature. Selecting the simplest protocol that meets the needs of the internetwork design and that is supported by the DDR routers is generally recommended.
4.5.5 Deactivating routing updates

In the topology displayed in Figure 1, the Central router is configured with a static route that points to the SOHO LAN, 172.24.2.0/24. The Central router is also configured for RIPv2, which is used as the core routing protocol in this example. Because the RIP network command accepts only classful addresses, the network 10.0.0.0 statement results in RIPv2 updates being sent on all of the Central router interfaces, including its BRI.

By default, RIP sends updates every 30 seconds. If the update qualifies as "interesting" traffic, Central will place a call every 30 seconds. When Central is already connected to SOHO, then the idle timer will be reset with each update. With the default dialer idle-timeout settings, a single update packet sent every 30 seconds would be enough to keep the link up forever. This would result in a very costly bill.

Typically, if a router is configured for dynamic routing and DDR, periodic routing updates should be prevented from establishing a call.

One solution is to configure the dialer list so that RIP traffic is not interesting. This solution is accomplished by using an access list. Since Central and SOHO are using static routes, there is no point in sending useless RIP updates across the dialup link. In such cases, the routing protocol should be configured to treat the DDR interface as a passive interface.

A passive interface listens to routing updates but does not send them. A passive interface is configured using the passive-interface command in router configuration mode. In Figure 2, Central should be configured so that RIP updates do not activate the DDR link.

```
Central(config)#ip route 172.24.2.0 255.255.255.0 bri 0
Central(config)#router eigrp 100
Central(config-router)# redistribute static
```
4.5.6 Snapshot routing

Usually, when connecting to a stub network, a combination of static and default routes used between dialup sites is all that is needed to maintain end-to-end connectivity. There are situations where neither of the link partners connects to a stub network. In these cases, it may be desirable to implement dynamic routing. Dynamic routing allows complex networks with redundant paths to automatically adapt to topology changes.

Snapshot routing is a method of dynamic routing that is optimized for use with dialer interfaces. When a router is configured for snapshot routing, the interval between updates is controlled. Therefore, a routing protocol, such as RIP, does not keep a link up constantly.

Snapshot routing works with the following distance-vector protocols:

- RIP for IP
- IGRP for IP
- Novell RIP and SAP for Novell IPX
- Routing Table Maintenance Protocol (RTMP) for AppleTalk
- Routing Table Protocol (RTP) for Banyan VINES

By default, these routing protocols send updates every 10 to 90 seconds. If a router considers these updates interesting, the DDR link may stay up indefinitely. If the router does not consider these updates interesting, then updates will not be delivered unless the dialup link is already established. Therefore, the routing protocol may be forced to declare routes as down and remove them from the routing table. Snapshot routing provides a solution to this dilemma.

Link-state routing protocols send periodic "hellos" to neighbors in addition to link-state update packets. Typically, hellos are exchanged between neighbors every five or ten seconds. Hellos are required in the operation of link-state protocols because they allow the routers to build relationships for the purpose of exchanging routes. Therefore, in a DDR environment, link-state protocols would trigger a call every few seconds. Since EIGRP relies on the exchange of hellos between neighbors, it cannot be used with
snapshot routing. On a network running OSPF, configure the OSPF on-demand circuit feature. Alternately, on a network that runs OSPF or EIGRP, use RIP or IGRP between DDR hosts, and then redistribute these routes into another routing protocol.

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

4.6.7 ISDN BRI configuration example

Figure 1 presents an ISDN BRI configuration scenario. The branch office router, BranchA, must be configured to use DDR over ISDN to dial into the Central office. However, the company does not want FTP or Telnet keeping the DDR link active. Also, once the first B channel reaches 50 percent load, the second B channel should be brought up, using MLP.

The service provider has assigned the following connection parameters to the branch office site:

- National ISDN-1 Switch
- SPIIDs: 51055512340001 and 51055512350001
- LDN 5551234 and 5551235

4.7.1 The show interface bri command

There are several important show and debug commands that can be used to monitor and troubleshoot ISDN operation. The show interface bri command displays information about the BRI D channel. The show interface bri command also displays information about one or more B channels, provided that the router is a TE1 and has a native BRI.

The example output displays "BRI0/0 is up, line protocol is up (spoofing)". Regardless whether an ISDN call is established or not, the BRI interface pretends to be up. This pretend state is called "spoofing". Spoofing is necessary because the router removes a route from its routing table if the route points to a "down" interface. If the BRI was allowed to report its status as "down", no routes using the BRI could be included in the routing table. If no routes using the BRI are in the routing table, then DDR cannot route packets to that interface in order to bring the link up.

Information on both B channels can also be displayed by using the show interface
The output of the `show interface bri [slot/port] 1 2` command shows that the B channels do not spoof their status. These lines will only show "up" if a call has been established.

A convenient way to display the operational status of the BRI and both B channels is to use the `show ip interface brief` command. Note that the output of this command shows the BRI as "up", when in fact, the interface is spoofing.

### 4.7.2 ISDN show commands

One of the most important `show` commands used with ISDN is `show isdn status`. This command displays ISDN status information for Layer 1, Layer 2, and Layer 3.

The output shown in Figure 4 was captured on a router while both B channels on the router were active. Notice that the Layer 2 information includes the TEI for each B channel, as well as an indication as to whether the SPIDs have been sent and accepted. At Layer 3, the two calls are active and both call types are "DATA".

The `show isdn status` command is especially useful when trying to track down the root of an ISDN connectivity problem. It can be seen that TEIs have successfully been assigned to each B channel. However, according to the output, the second B channel has sent its SPID to the ISDN switch and was rejected. The most likely cause of this problem is that the router has been configured with the wrong SPID.

The `show isdn history` command helps gather information on previous calls, not just those that are currently active. This command will output information on calls that have occurred during the past 15 minutes.

As with any dialer interface, the `show dialer` command will prove to be an invaluable monitoring and troubleshooting tool for ISDN interfaces. Figure 4 displays `show dialer` output during an established call on the first B channel. The second B channel is idle.