MODULE 4

Wide-Area Networking

CHAPTER 16

Introduction to Serial Connections

Objectives

Upon completion of this chapter, you will be able to:

Describe and distinguish the types and attributes of serial communication on WANs

Describe how WAN communication works

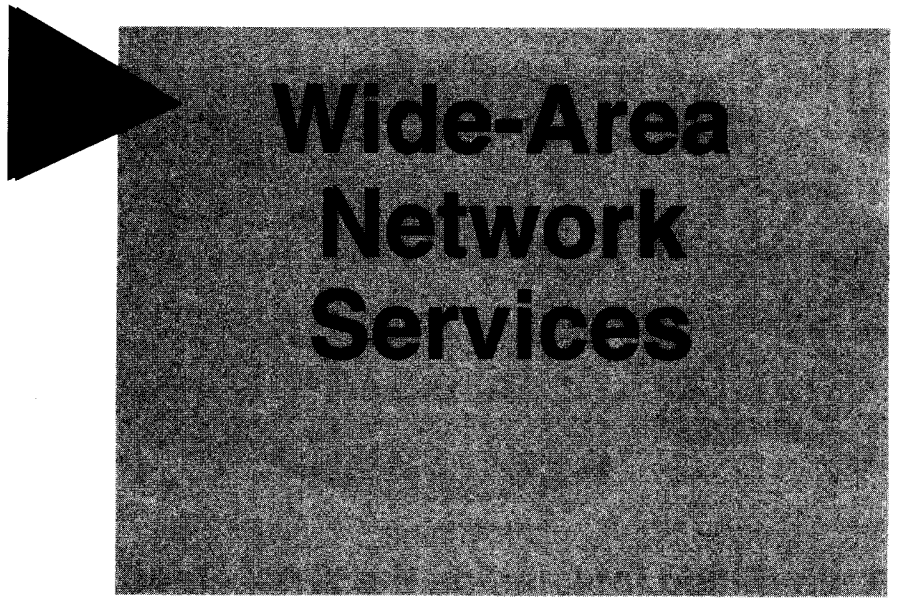
Identify Point-to-Point Protocol operations to encapsulate WAN data on Cisco routers

Identify dial-on-demand routing processes as a signaling trigger for WAN data calls on Cisco routers

This chapter discusses how wide-area networks are set up, how a user subscribes to phone services for the network, and what a WAN frame looks like. It also presents the Point-to-Point Protocol (PPP) and explains dial-on-demand routing (DDR).

Sections:

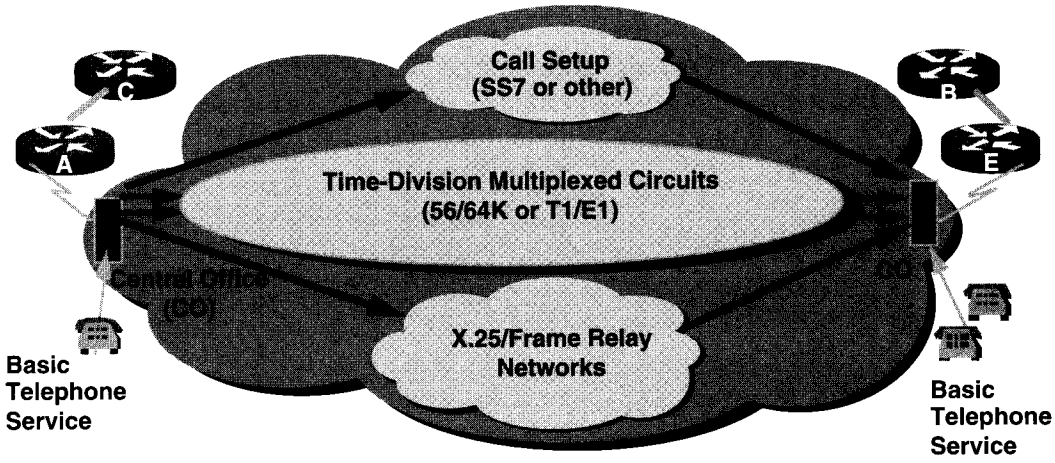
- Wide-Area Network Services
- Point-to-Point Protocol
- Dial-on-Demand Routing
- Answers to Exercises



3

Wide-Area Network Services

An Overview of Wide-Area Services



- **A simplified look inside the WAN cloud**
- **The router also uses a WAN central office**

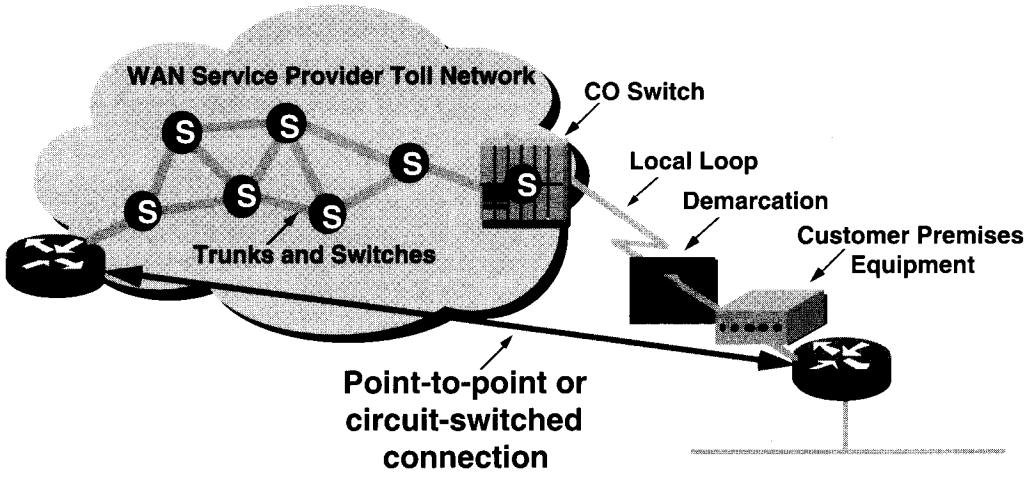
4

A wide-area network (WAN) is different from a local-area network. With a WAN, you must subscribe to an outside WAN provider to use network resources that your organization does not own. Basic telephone service is the most commonly used WAN service. Telephone service and data service routed from the customer premises interface with the service provider's cloud at a central office (CO).

An overview of the WAN cloud organizes WAN provider services into three main types:

- Call setup service—Sets up and clears calls between telephone users. Also called signaling, call setup uses a separate telephone channel not used for other traffic. The most commonly used call setup is Signaling System number 7 (SS7). It uses telephone control messages and signals between the transfer points along the way to the called destination.
- Time-division multiplexing (TDM)—Information from multiple sources has bandwidth allocation on a single media. Circuit switching uses signaling to determine the call route, which is a dedicated path between the sender and the receiver. By multiplexing traffic into fixed time slots, TDM avoids congested facilities and variable delays. Basic telephone service and Integrated Services Digital Network (ISDN) use TDM circuits.
- X.25 or Frame Relay service—Information contained in packets or frames shares nondedicated bandwidth. X.25 packet switching uses Layer 3 routing with sender and receiver addressing contained in the packet. By using virtual circuits (VCs), X.25 avoids delays for call setup. Frame Relay uses Layer 2 identifiers and permanent virtual circuits (PVCs). By streamlining functions, Frame Relay adjusts its bandwidth to handle bursty traffic.

Interfacing WAN Service Providers



- **Provider assigns connection parameters to subscriber**

5

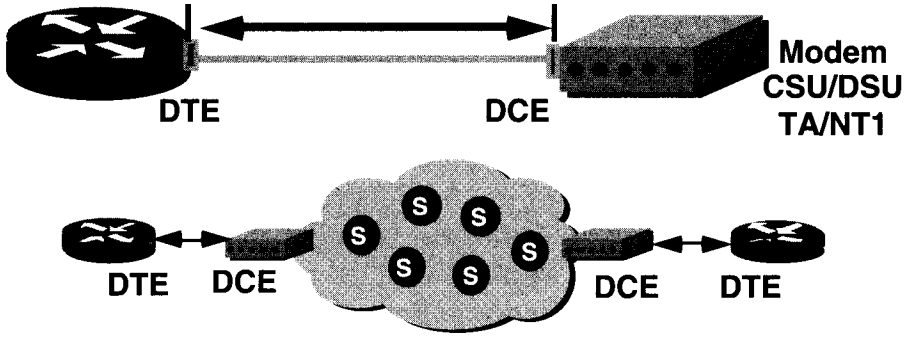
When your organization subscribes to an outside WAN provider for network resources, the provider assigns your organization the parameters for connecting WAN calls. Your organization makes connections to destinations as point-to-point calls. These are the most commonly used terms for these main parts.

- Customer premises equipment (CPE)—Devices physically located on the subscriber's premises. Includes both devices owned by the subscriber and devices leased to the subscriber by the service provider.
- Demarcation (or demarc)—The juncture at which the CPE ends and the local loop portion of the service begins. Often occurs at a telecommunication closet.
- Local loop (or "last-mile")—Cabling (usually copper wiring) that extends from the demarc into the WAN service provider's central office.
- Central office (CO)—A switching facility that provides the nearest point of presence for the provider's WAN service. Inside the long distance toll network are several types of central offices.
- Toll network—The collective switches and facilities (called trunks) inside the WAN provider's cloud. The caller's traffic may cross a trunk to a primary center, then go to a sectional center, and then to a regional- or international-carrier center as the call goes the long distance to its destination. Switches operate in provider offices with toll charges based on tariffs or authorized rates.

Subscriber to Provider Interface

Data Terminal Equipment
End of the user's device on the WAN link

Data Circuit-Terminating Equipment
End of the WAN provider's side of the communication facility



- **DTE/DCE—The point where responsibility passes**

6

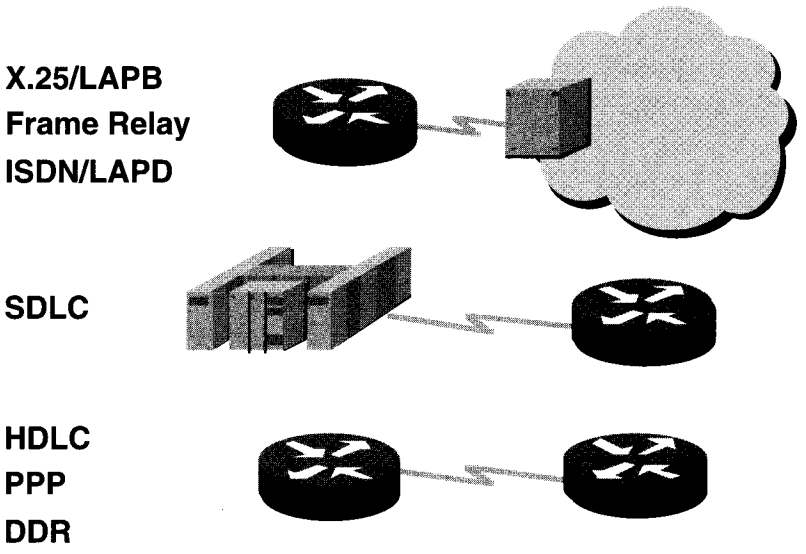
A key interface in the customer premises occurs between the data terminal equipment (DTE) and the data circuit-terminating equipment (DCE).

Typically, DTE is the router where the packet switching application resides. The DCE is the device used to convert the user data from the DTE into a form acceptable to the WAN service's facility. In the graphic, the DCE is the attached modem, channel service unit/data service unit (CSU/DSU), or terminal adapter/Network Termination 1 (TA/NT1).

Data communication over WANs interconnects DTEs so they can share resources with each other over a wide area. The WAN path between the DTEs is called the link, circuit, channel, or line. The DCE primarily provides the interface of the DTE into the communication link in the WAN cloud. The DTE/DCE interface acts as a boundary where responsibility for the traffic passes between the WAN subscriber and the WAN provider.

The DTE/DCE interface uses one of the various protocols available. These protocols establish the codes that the devices use to communicate with each other. This communication determines how call setup operates and how user traffic crosses the WAN.

Using WAN Services with Routers



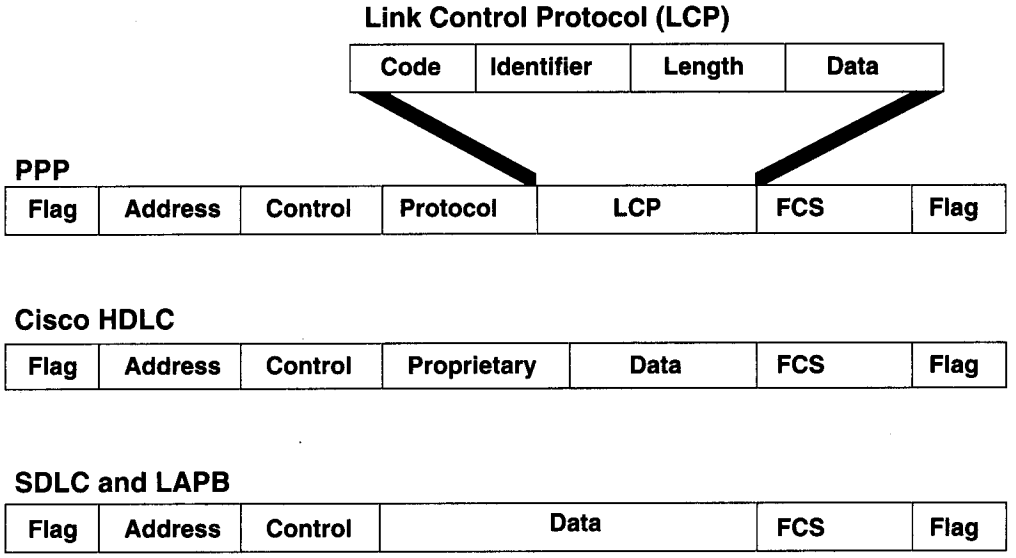
7

You can access three forms of WAN services with Cisco routers:

- The first form uses switched or relayed services. A special device interfaces to a service provider's cloud. Examples of this form of WAN include X.25, Frame Relay, and ISDN. Chapters on each of these WAN services follow in this module.
- The second form of WAN service provides an interface front end to the IBM enterprise data center computers. This form of WAN uses Synchronous Data Link Control (SDLC) for the point-to-point or point-to-multipoint connection of remote devices to the central mainframe. This topic is covered in Cisco's System Network Architecture (SNA) configuration courses.
- With the third form, you can access the services of WAN providers using protocols that connect peer devices. This form uses High-Level Data Link Control (HDLC) or PPP encapsulation on the peer devices. An introduction to PPP follows this section.

  This third form of WAN access can use DDR as a trigger for the Cisco router to make a WAN call. For example, a router uses DDR statements when local user traffic needs to set up an ISDN call over a WAN so it can access a remote network. An introduction to DDR follows later in this chapter.

WAN Frame Format Summary



- **Formats assume framing on dedicated WAN facilities**

8

The frame formats for SDLC and Link Access Procedure, Balanced (LAPB) are very similar. SDLC is IBM's bit-synchronous data-link protocol that is a primary ancestor for serial framing. It supports legacy IBM networks.

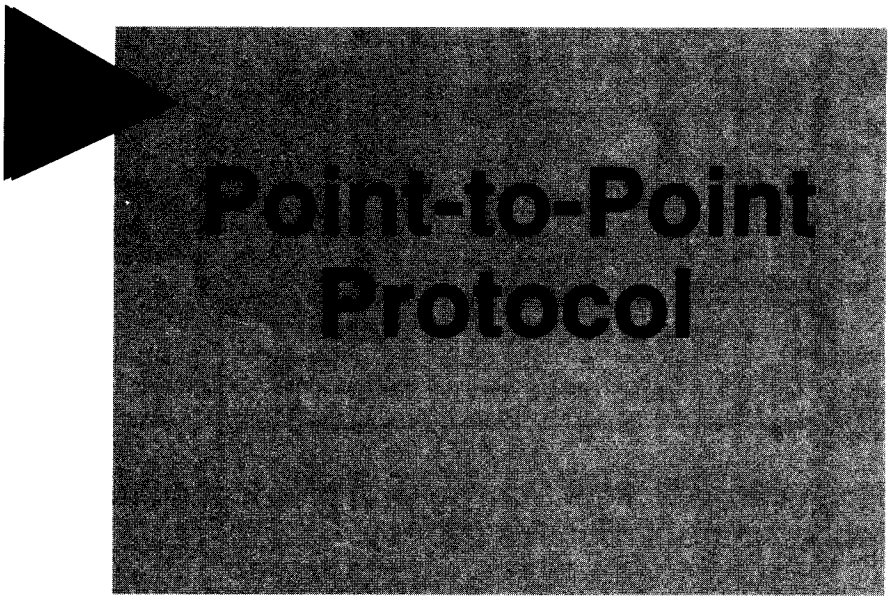
LAPB, used by X.25, a nonproprietary standard from ITU-T (formerly the CCITT), is derived from HDLC. HDLC is the popular ISO-standard bit-oriented data-link protocol that encapsulates data on synchronous serial data links. Frame Relay also uses a variation of HDLC.

HDLC does not inherently support multiprotocols on a single link because it does not have a standard way to indicate which protocol it is carrying. The Cisco HDLC frame uses a proprietary type field that acts as a protocol field. This makes it possible for multiple network-layer protocols to share the same serial link.

PPP extends the basic SDLC frame by incorporating a protocol field. The protocol field identifies the protocol encapsulated in the information field of the frame.

The Link Control Protocol (LCP) used by PPP provides a method of establishing, configuring, maintaining, and terminating the point-to-point connection. LCP serves much the same function as the 802.2 logical link control (LLC) in the LAN protocols.

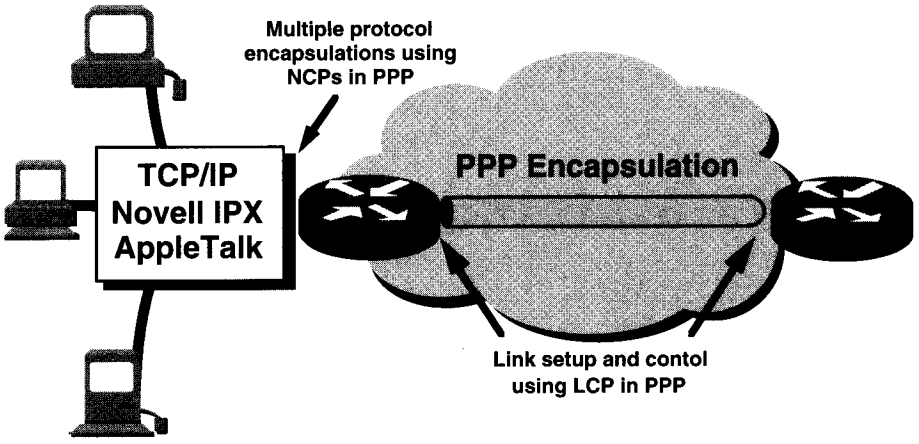
This course deals mainly with the WAN frame formats for PPP and HDLC. Serial connections use WAN framing that is similar. However, field differences in the framing types makes it necessary to specify the framing needed unless the serial line default Cisco HDLC is sufficient.



9

Point-to-Point Protocol

An Overview of PPP



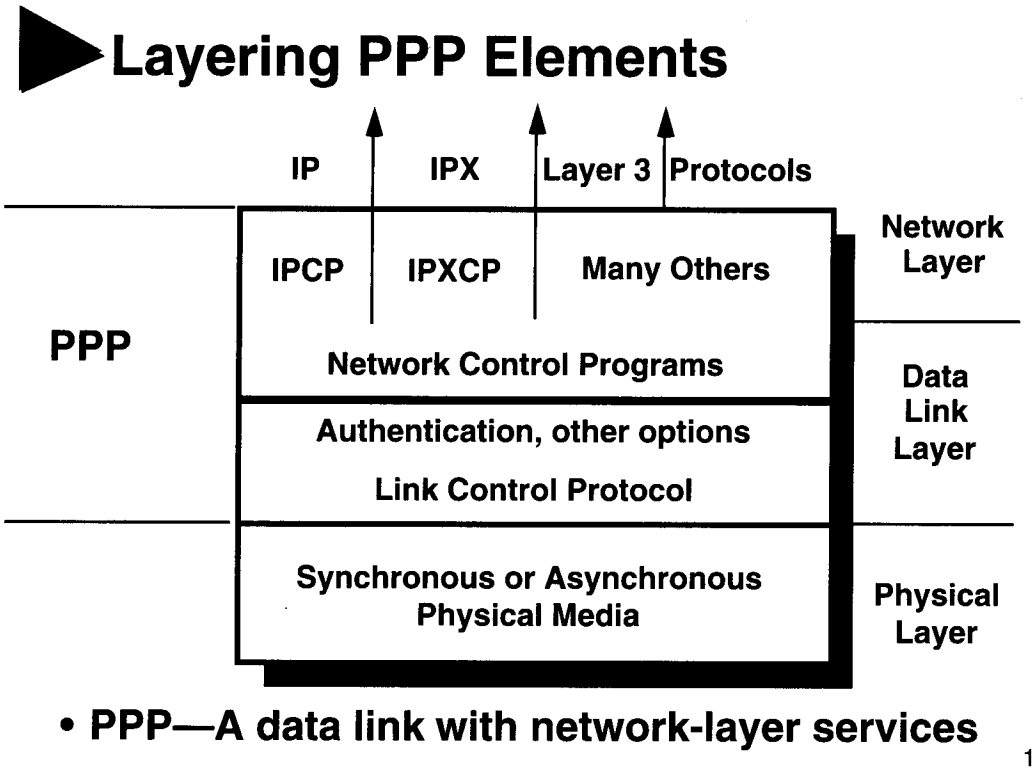
- **PPP can carry packets from several protocol suites using Network Control Programs (NCPs)**
- **PPP controls the setup of several link options using LCP**

10

Developers on the Internet designed PPP to make the connection for point-to-point links. Originating with RFCs in the late 1980s, PPP replaces limited or proprietary protocols for asynchronous or synchronous dial-up connections.

PPP uses its Network Control Programs (NCPs) component to encapsulate multiple protocols. This use of NCPs surpasses the limits of PPP's predecessor Serial Line IP (SLIP, which could only set up transport for IP packets).

PPP uses another of its major components, the LCP, to negotiate and set up control options on the WAN data link.



PPP uses a layered architecture. With its lower-level functions, PPP can use synchronous physical media like those that connect ISDN and asynchronous physical media like those that use basic telephone service for modem dial-up connections.

PPP offers a rich set of services that control setting up a data link. These services are options in LCP and are primarily negotiation and checking frames to implement the point-to-point controls an administrator specifies for the call.

With its higher-level functions, PPP carries packets from several network-layer protocols in NCPs. These are functional fields containing standardized codes to indicate the network-layer protocol type that PPP encapsulates.

PPP LCP Configuration Options

Feature	How It Operates	Protocol
Authentication	Require a password Perform Challenge Handshake	PAP CHAP
Compression	Compress data at source; reproduce data at destination	Stacker or Predictor
Error Detection	Monitor data dropped on link Avoid frame looping	Quality Magic Number
Multilink	Load balancing across multiple links	Multilink Protocol (MP)

12

RFC 1548 describes PPP operation and LCP configuration options. Cisco routers that use PPP encapsulation include the LCP options shown in the table.

- Authentication options require that the calling side of the link enter information to help ensure the caller has the network administrator's permission to make the call. Peer routers exchange authentication messages. Two alternatives are:
  - Password Authentication Protocol (PAP)
  - Challenge Handshake Authentication Protocol (CHAP)
- Compression options increase the effective throughput on PPP connections by reducing the amount of data in the frame that must travel across the link. The protocol decompresses the frame at its destination.

  Two compression protocols available in Cisco routers are Stacker and Predictor.
- Error-detection mechanisms with PPP enable a process to identify fault conditions. The Quality and Magic Number options help ensure a reliable, loop-free data link.
- Cisco IOS Release 11.1 and later support multilink PPP. This alternative provides load balancing over the router interfaces that PPP uses.

  Packet fragmentation and sequencing, as specified in RFC 1717, splits the load for PPP and sends fragments over parallel circuits. In some cases, this "bundle" of multilink PPP pipes functions as a single logical link, improving throughput and reducing latency between peer routers.

Configuring PPP

Router (config-if) #

encapsulation ppp

- **Defines encapsulation type as PPP**

Router (config-if) #

ppp authentication pap

- **Sets password checking for incoming calls**

Router (config-if) #

ppp authentication chap

- **Forces incoming calls to answer password challenges**

Router (config) #

username *name* password *secret-pwd*

- **Sets host name and password for call verification**

13

The commands shown in the graphic relate to PPP configurations most commonly used for ISDN on Cisco routers.

Note The administrator may use either PAP or CHAP, but not both, on a PPP link. PAP uses the exchange of clear-text passwords between the calling and called sides of the link. Alternately, CHAP is a more sophisticated process that authenticates the caller without disclosing the password on the link. CHAP is less vulnerable to line taps and is generally preferred because it provides better security.

PPP Configuration Example

encapsulation ppp
ppp authentication chap

14

In the example:

Command	Description
encapsulation ppp	Defines PPP encapsulation.
ppp authentication chap	Defines CHAP as password authentication method.

The **username** ***name*** **password** ***secret-pwd*** command could also be used in this example. This command enables the secret password feature of CHAP.

When CHAP is enabled, a remote device (a PC, workstation, or access server) attempting to connect to the local access server is requested, or "challenged," to respond. The challenge consists of an ID, a random number, and either the host name of the local access server or the name of the user on the remote device. This challenge is transmitted to the remote device.The required response consists of two parts:

- An encrypted version of the ID, a secret password (or secret), and the random number
- Either the host name of the remote device or the name of the user on the remote device

When the local access server receives the challenge response, it verifies the secret by looking up the name given in the response and performing the same encryption operation. The secret passwords must be identical on the remote device and the local access server. By transmitting this response, the secret is never transmitted, thus preventing other devices from stealing it and gaining illegal access to the system. Without the proper response, the remote device cannot connect to the local access server.

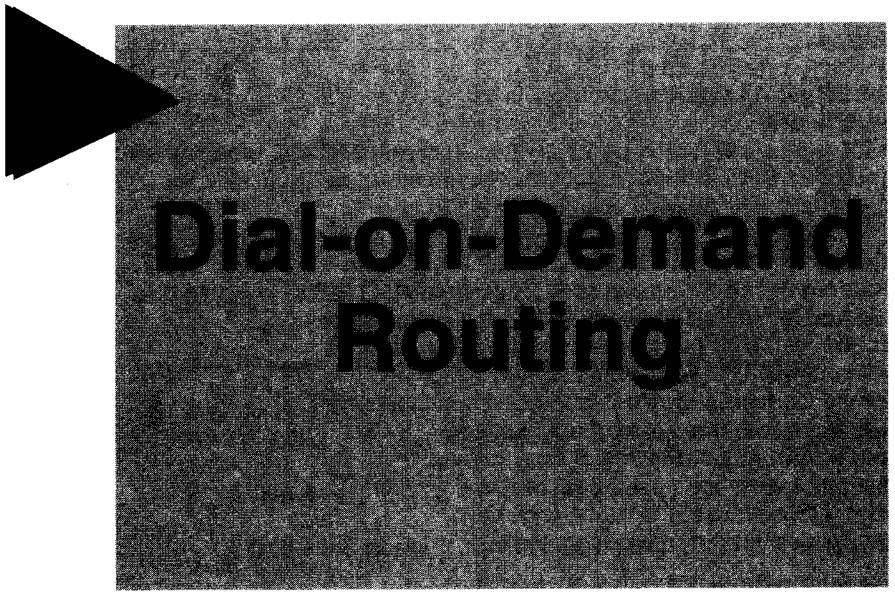
Monitoring PPP

```
Router# show interface b0 b 1
BRI0: B-Channel 1 is up, line protocol is up
  Hardware is BRI
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive not set
  lcp     = OPEN     multilink = OPEN
  ipcp    = OPEN
  Last input 0:05:51, output 0:05:52, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Output queue: 0/64/0 (size/threshold/drops)
     Conversations  0/1 (active/max active)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     15 packets input, 804 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      14 packets output, 806 bytes, 0 underruns
     0 output errors, 0 collisions, 19 interface resets, 0 restarts
     0 output buffer failures, 0 output buffers swapped out
     1 carrier transitions
```

15

When PPP is configured, you can check its LCP and NCP states using the **show interfaces** command.

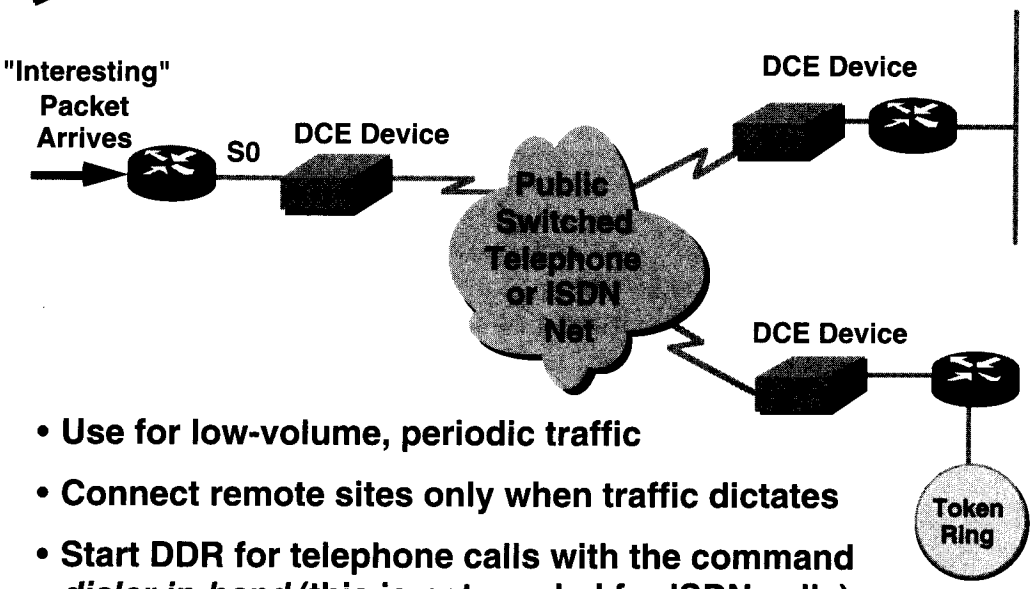
In the example, the administrator used this command to monitor the Basic Rate Interface (BRI). The multilink option is enabled.



16

Dial-on-Demand Routing

An Overview of DDR



- **Use for low-volume, periodic traffic**
- **Connect remote sites only when traffic dictates**
- **Start DDR for telephone calls with the command *dialer in-band* (this is not needed for ISDN calls)**

17

With dial-on-demand routing, the router opens the wide-area connection only when there is traffic that needs to be transmitted. The context for using DDR involves infrequent or intermittent traffic to and from remote sites. DDR uses a WAN facility such as asynchronous, dial-in access or ISDN. Compared to the traffic using LAN or campus-based networking, the traffic that uses DDR is typically low volume and periodic.

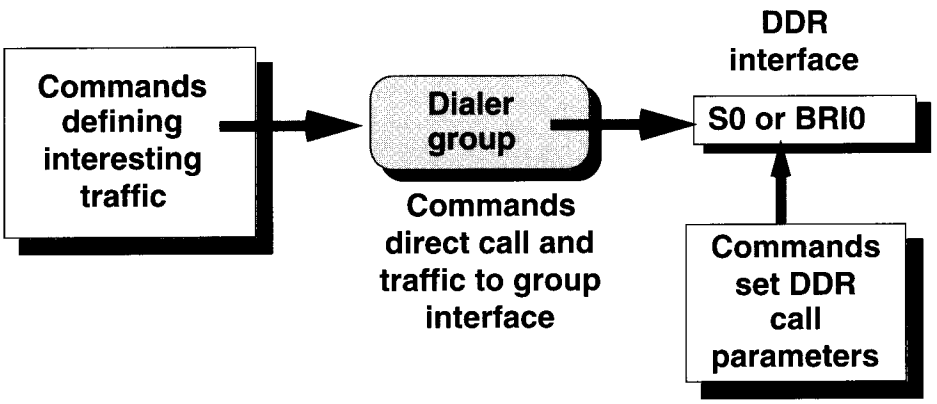
There are two ways to start DDR. If you will be using a public switched telephone service, start DDR by entering the **dialer in-band** command. This sets up the proper call operations between the router and a DCE device such as an external modem. The call setup uses the same bandwidth that data will use after the call is made.

If you are using an ISDN service, there is no need for the **dialer in-band** command. As you will see later, the ISDN call setup uses an out-of-band channel that is different than the channels that bear data. The ISDN alternative is featured in this course.

To identify the traffic that should be transmitted, you specify the packets that the DDR processes on the router will interpret as "interesting" traffic.

Specify static routes to the remote sites on links that DDR will use. This prevents routing updates across the DCE and over the Public Switched Telephone Network (PSTN) cloud. Unlike routing updates on a LAN or campus, WAN traffic increases the charges billed by the WAN service provider.

DDR Configuration Overview



- **Define interesting traffic to trigger call**
- **Direct call and traffic to dialer-group interface**
- **Make and control call with DDR-configured parameters**

18

The previous page had a high-level introduction to DDR. This page provides a high-level summary of the configuration steps to follow when configuring DDR.

- Enter configuration commands that indicate which protocol packets constitute interesting traffic to initiate the call. Choose between two approaches:
  - — Indicate that all packets in a specified protocol are sufficient to make the call.
  - — Set access list statements to identify the source and destination addresses and choose specific protocol selection criteria for initiating the call.
- Establish the interfaces where the DDR call initiates. This step designates a dialer group. The dialer group associates the results of the first step to the router's interfaces.
- Include information about the call. This information might include:
  - — The carrier-provided number to use when initiating the call sequence.
  - — One or more configuration-parameter statements to synchronize the router's calls with operational requirements of the CO switch. Examples include:
    - Should bandwidth be set to 56 kbps or is the default 64 kbps appropriate?
    - Does the switch require any pauses or other adjustments for call processing?
    - How long should the line be idle before dropping the call?

Define Interesting Traffic for DDR

Router (config) #

dialer-list *dialer-group* list *access-list-number*

- **Sets number for the dialer group used by DDR interface(s)**
- **Assigns previous access list expressions to dialer group**

OR

Router (config) #

dialer-list *dialer-group* protocol *protocol-name*
[permit | deny | list *access-list-number*]

- **Triggers call by protocol or protocol and access list**
- **Assigns previous access list expressions to dialer group used by DDR interface(s)**

19

DDR uses two ways to specify interesting packets that trigger the dialer to make a call.

The first way uses the **dialer-list list** global command. It applies an access list to a specified dialer group. The access list specifies any IP or IPX access list including standard, extended, and IPX service access point (SAP) access lists.

The second way to specify interesting packets uses the **dialer-list protocol** command. With this method, you can specify a protocol or a combination of protocol and a previously defined access list.

dialer-list protocol Command	Description
dialer-group	Specifies the number of the dialer group. Later, this dialer-group number associates specific interfaces with the dialer list.
protocol-name	Specifies the protocol for packets to be considered for DDR. Choices include ip, ipx, appletalk, decnet, and vines.
permit | deny	Optional entry to specifically permit or deny an entire protocol for DDR; if field is not entered, traffic is permitted by default.
list	Specifies that an access list will define permit or deny based on granularity finer than the entire protocol.
access-list-number	The access list number specified for the protocol. For example, access list 120 specifies an extended IP access list.

Place Interface in the Dialer Group

Router (config-if) #

dialer-group *group-number*

- **Make the interface part of a group of interfaces**
- **Associate interface with the dialer list**
- **For interesting packets, DDR will direct call and packets to appropriate interface in the dialer group**

20

Use the **dialer-group** command to assign an interface to a dialer access group. This connects the interface you are configuring to access list statements that identify interesting protocol traffic.

dialer-group Command	Description
group-number	Specifies the number of the dialer group to which the interface belongs. The group number can be an integer from 1 to 10.

When interesting packets arrive (as specified by the **dialer-list** command), DDR will trigger a call to the appropriate dialer-group interface. When the call setup finishes, DDR routes the interesting packets out this interface.

Set DDR Call Parameters with Map

Router (config-if) #

dialer map *protocol next-hop-address* [name *hostname*] [speed 56|64] [broadcast] [*dial-string*]

- **Defines how to reach a DDR destination**
  - **Recipient's protocol address**
  - **(Optional) Host name of remote system**
  - **(Optional) Line speed for TDM circuit**
  - **(Optional) Indicates broadcasts are forwarded**
  - **(Optional) Phone number of next hop sent to the dialing device for interesting traffic**

21

Use the **dialer map** command to define one or several dial-on-demand numbers for a particular interface.

dialer map Command	Description
protocol	Must be IP, IPX, or AppleTalk.
next-hop-address	Address of the next-hop router.
name	An identification generally used for PPP authentication from PAP or CHAP or some other calling-line identifier of the far-end router. It can also help associate a number from one provider coming in from another provider (for example, two PTTs having different identification numbers).
dial-string	ISDN dial string sent to the V.25 bis DCE device when packets with the specified next-hop address are received. The character string passed to the V.25 bis device comes from the WAN service provider. It can be any number or format that works for the specific provider.

The **dialer map** command must be used with the **dialer-group** command and its associated access list to initiate dialing.

Other Call Control Parameters

Router (config-if) #

dialer wait-for-carrier-time *seconds*

- **Specifies time to wait for carrier to come up**

Router (config-if) #

dialer idle-timeout *seconds*

- **Specifies idle time before circuit disconnect**

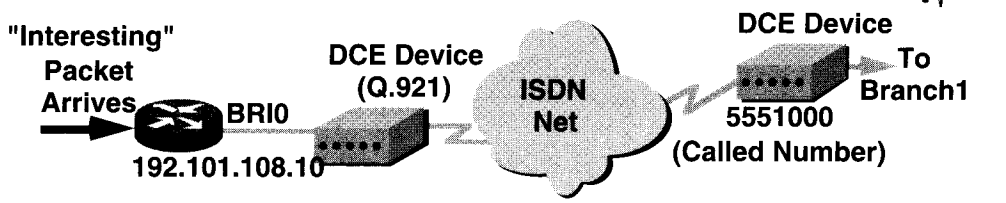
22

The **dialer wait-for-carrier-time** command specifies the number of seconds the router waits for the WAN service provider to come up when a call initiates. Because the time for call initiation can vary, a larger number of seconds to wait can accommodate the delay (for example, making worldwide interconnections).

The **dialer idle-timeout** command specifies the number of idle seconds before a call is disconnected. When an interface in a dialer group receives an interesting packet, it resets the idle seconds counter. The call is not disconnected until the idle-seconds threshold on the dialer-group interface is reached.

DEFAULT = 2 MINUTES.

DDR Example for ISDN




```
! (Prior global configuration commands specify switch and static routes)
access-list 111 deny ip any 255.255.255.255 0.0.0.0
access-list 111 permit ip any  0.0.0.0 255.255.255.255
dialer-list 1 protocol ip list 111
!
interface bri 0
ip address 192.101.108.10 255.255.255.0
dialer-group 1
!
dialer map ip 192.101.108.10 name branch1 speed 64 5551000
dialer idle-timeout 300
```

23

In the example, DDR will operate for ISDN. For the ISDN Basic Rate Interface (BRI) call, the configuration statements assume that the ISDN details of switch type and static routes to the destination have already been set up.

Command	Description
access-list 111 deny ip any 255.255.255.255 0.0.0.0	Denies packets using IP from any source to the specific destination of 255.255.255.255. No IP broadcast will be interesting traffic that causes a DDR call.
access-list 111 permit ip any any	Permits packets using IP from any other source to any other destination to be interesting for causing a DDR call.
dialer-list 1 protocol ip list 111	Assigns the dialer group number 1 as the dialer group that the dialer-group interfaces will use for IP traffic calls triggered by access list 111.
dialer-group 1	Makes BRI0 part of the dialer group. Calls triggered by access list 111 can use this dialer-group 1 interface.
dialer map ip 192.101.108.10 name branch1 speed 64 5551000	Sets the BRI0 call parameters: Use 192.101.108.10 as the port out to a static route to branch1. Use 64 kbps and the dial string 5551000 to make the BRI call.
dialer idle-timeout 300	Set an optional call parameter for BRI0: If the idle seconds threshold on BRI reaches 300 seconds, DDR will disconnect the call.

Summary

A WAN subscriber must know how to interface customer premises equipment to the provider service

Mapping associates the Layer 3 address with the WAN media-dependent address

PPP sets data-link encapsulation capable of transmitting packets from multiple protocols

DDR enables "as-needed-only" use of expensive WAN links by triggering calls based on traffic-type lists

Exercise: Serial Connections

Problem 1

Objective: Describe and distinguish the types and attributes of serial communication on WANs.

Write the letter for the term that most closely matches the definition.

Terms:

A) Call setup service

B) Time-division multiplexing (TDM)

C) X.25 or Frame Relay service

Definitions:

____ Uses a separate channel for control messages between transfer points to a called destination.

____ Statistically allocates bandwidth on a single channel to multiple circuits.

____ Also known as signaling.

____ Uses fixed time slots to eliminate congestion.

____ Packets of information share a nondedicated channel.

____ Sets up and clears calls between users.

____ Route is a dedicated path between sending location and receiving location.

____ Uses virtual circuits to avoid call setup delays.

Problem 2

Objective: Describe how WAN communication works.

1. Any telecommunication equipment located at the subscriber's premises is called _____. This equipment may include both _____ and _____.

2. At the interface where responsibility for traffic passes from the WAN subscriber to the WAN provider, a router is most often a _____.

3. What are the three forms of WAN services described in the chapter that you can access with Cisco routers?

A)

B)

C)

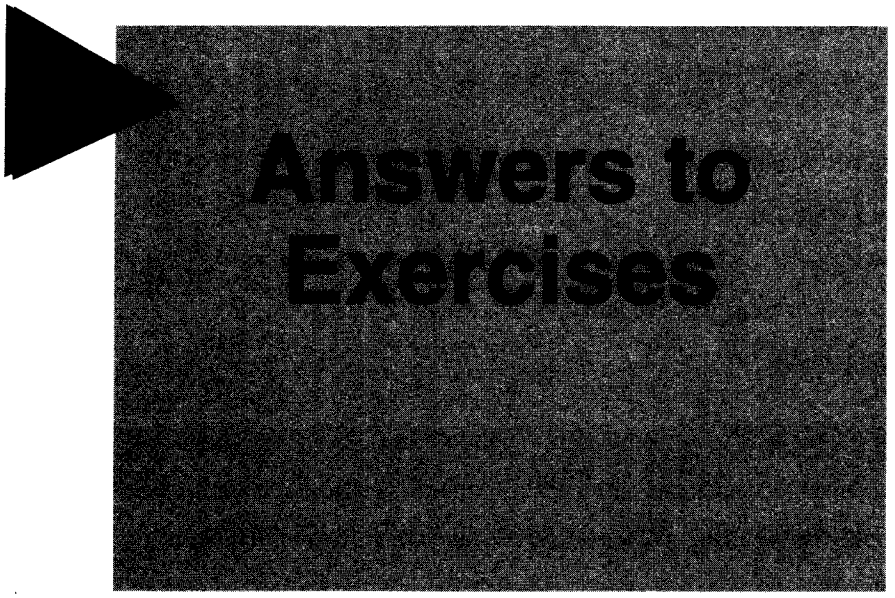
Problem 3

Objective: Identify Point-to-Point Protocol operations to encapsulate WAN data on Cisco routers.

Objective: Identify dial-on-demand routing processes as a signaling trigger for WAN data calls on Cisco routers.

Place a check in the column indicating whether the description refers to PPP or DDR.

PPP	DDR	Description
		Relies on static routing entries.
		Uses Password Authentication Protocol (PAP).
		Offers compression to increase effective throughput.
		Offers Magic Number option to improve data reliability.
		Offers multilink option to load balance transmissions across a communication bundle.
		Initiates call based on interesting traffic.
		Defines a dialer group.
		Uses Challenge Handshake Authentication Protocol (CHAP).
		Uses access lists to determine whether to initiate a call.
		Offers waiting period for carrier or disconnect.
		Offers authentication to verify approval to make or receive a call.



27

Answers to Exercises

Exercise: Serial Connections

Problem 1

A Uses a separate channel for control messages between transfer points to a called destination.

B Statistically allocates bandwidth on a single channel to multiple circuits.

A Also known as signaling.

B Uses fixed time slots to eliminate congestion.

C Packets of information share a nondedicated channel.

A Sets up and clears calls between users.

B Route is a dedicated path between sending location and receiving location.

C Uses virtual circuits to avoid call setup delays.

Problem 2

1. Any telecommunication equipment located at the subscriber's premises is called *customer premises equipment (CPE).* This equipment may include both *data terminal equipment (DTE)* and *data circuit-terminating equipment (DCE).*

2. A router is most often a *DTE.*

3. What are the three forms of WAN services you can access with Cisco routers?

A) *Switched or relay services*

B) *Front end to an IBM enterprise data center computer*

C) *Connection between peer devices*

Problem 3

PPP	DDR	Description
	√	Relies on static routing tables.
√		Uses Password Authentication Protocol (PAP).
√		Offers compression to increase effective throughput.
√		Offers Magic Number option to improve data reliability.
√		Offers multilink option to load balance transmissions across a communication bundle.
	√	Initiates call based on interesting traffic.
	√	Defines a dialer group.
√		Uses Challenge Handshake Authentication Protocol (CHAP).
	√	Uses access lists to determine whether to initiate a call.
	√	Offers waiting period for carrier or disconnect.
√		Offers authentication to verify approval to make or receive a call.

CHAPTER 17

Configuring ISDN BRI

Objectives

Upon completion of this chapter, you will be able to perform the following tasks:

State a relevant use and context for ISDN networking

Identify ISDN protocols, function groups, reference points, and channels

Relate Point-to-Point Protocol (PPP) and dial-on-demand routing (DDR) functions to ISDN

Describe Cisco's implementation of ISDN BRI

Configure an ISDN call, open a circuit, and pass data over an interface

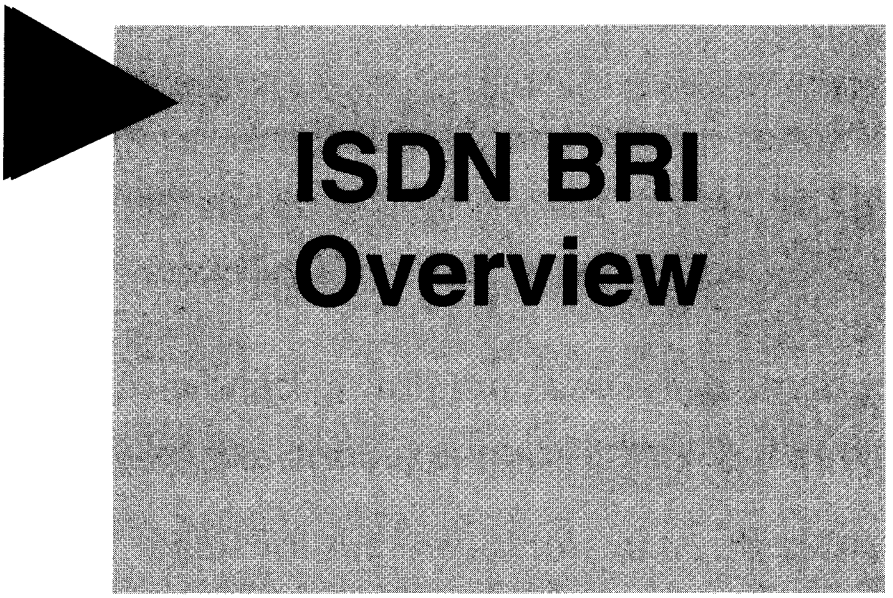
Monitor and analyze ISDN operation through the router

2

This chapter discusses the concepts of ISDN Basic Rate Interface (BRI) and how to configure the protocol. It presents an explanation of general ISDN services and explains how to obtain those services. It explains how to do global, interface, and optional feature configuration and how to monitor ISDN operation.

Sections:

- ISDN BRI Overview
- Configuring BRI



3

ISDN BRI Overview

Using ISDN Services

- **Uses higher-quality end-to-end digital facilities**
- **Sets up call faster than basic telephone service**
- **Carries varied feeds (for example, packets, voice, video)**
- **Meets demand for telecommuting bandwidth**
- **Improves Internet response (especially for WWW)**

4

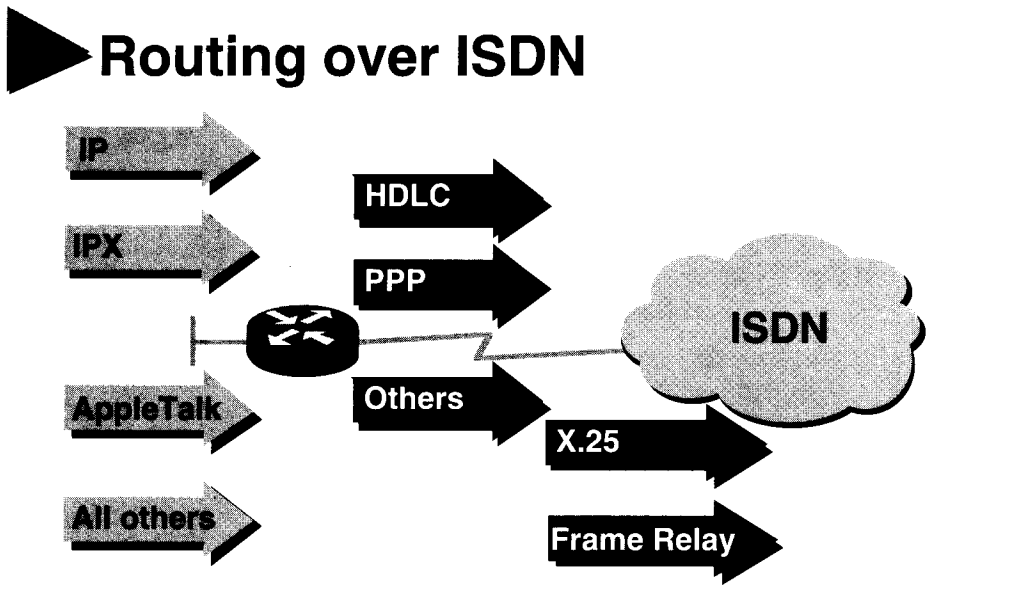
Integrated Services Digital Network (ISDN) is a complex call processing system that allows telephone networks to carry voice, data, and other source material in the same all-digital communication stream.

The product features much faster call setup using out-of-band signaling than modem connections. For example, a duration of less than 1 second can be sufficient to make some ISDN calls.

Once a call is up, ISDN can carry a variety of user-traffic feeds. The ISDN model shows ISDN providing access to all-digital facilities for video, telex, packet-switched data, and enriched telephone net services.

ISDN users access bearer (B) channel services at 64 kbps—much faster than common modem alternatives of 14.4 kbps. With multiple B channels, ISDN offers users more bandwidth on WANs than they receive with a leased line at 56 kbps in North America or 64 kbps in much of the rest of the world.

ISDN is fast becoming the transport of choice for applications using remote connectivity, access to the Internet, and the World Wide Web (WWW). Before the tremendous growth in these applications, many in the United States believed ISDN was a solution looking for a problem.



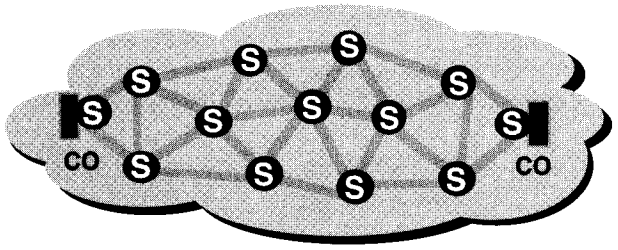
Once an ISDN call has been established, the router can use an ISDN cloud to carry any of the network-layer protocols supported by the Cisco IOS software to multiple destinations.

As its configured encapsulation, ISDN defaults to High-Level Data Link Control (HDLC). Alternately, a network administrator can select PPP. This choice can enable the PPP Challenge Handshake Authentication Protocol (CHAP), a popular, standards-based method for call screening. Among the other encapsulations for end-to-end ISDN is Link Access Protocol on the D Channel (LAPD).

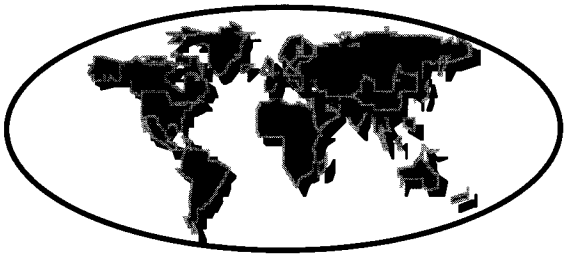
Although the ISDN call can statistically multiplex packets from several higher-layer protocols, ISDN interfaces allow only a single encapsulation type.

If the end-to-end path for user traffic interconnects with an X.25 or Frame Relay service, the administrator specifies the WAN encapsulation choices for these two services that will use the ISDN interface. This selection facilitates internetworking between the traffic passed from the ISDN cloud to these other WAN services.

Obtaining ISDN Services



- **Many providers and switch types**



- **Services vary by regions and countries**

6

Because ISDN originated in the research forums of CCITT and Bell Labs, developers planned a model for integrated services that users would access on a limited set of standard, multipurpose, user-to-network interfaces.

However, ISDN implementation does not guarantee seamless, end-to-end connectivity. ISDN providers use a variety of different switch types for their ISDN services. Services offered by the national Post, Telephone, and Telegraphs (PTTs) or other carriers vary considerably from nation to nation or region to region.

The good news is that ISDN services worldwide are increasing their offerings while decreasing their prices. The bad news is that you must be aware of the switch types used at the central office (CO) of your network. You specify this during configuration so your router can place ISDN network-level calls and send data. Following is a sample of countries and the ISDN switch types you are likely to encounter in your provider's ISDN cloud.

Country	Switch Type
United States and Canada	AT&T 5ess and 4ess; Northern Telecom DMS-100
France	VN2, VN3
Germany	1TR6
Australia	TS-013
Japan	NTT
United Kingdom	Net3 and Net5

ISDN Protocols

Issue	Protocols	Key Examples
Telephone network and ISDN	E-series	E.163—International telephone numbering plan E.164—International ISDN addressing
ISDN concepts, aspects, and interfaces	I-series	I.100 series—Concepts, structures, terminology I.400 series—User-Network Interfaces (UNIs)
Switching and signaling	Q-series	Q.921—LAPD (Link Access Procedure on the D channel) Q.931—ISDN network layer between terminal and switch

- **Standards from the ITU (CCITT)**

7

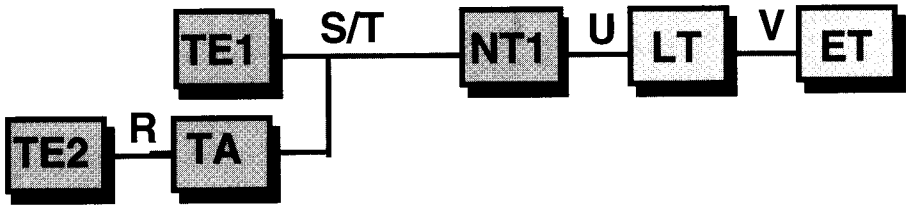
Work on standards for ISDN began in the late 1960s. A comprehensive set of ISDN recommendations was published in 1984 and is continuously updated by CCITT—now the International Telecommunication Union Telecommunication Standardization Sector (ITU-T). ITU-T groups and organizes the ISDN protocols according to general topic areas.

- Protocols that begin with "E" recommend telephone network standards for ISDN. For example, the E.164 protocol describes international addressing for ISDN.
- Protocols that begin with "I" deal with concepts, terminology, and general methods. The I.100 series includes general ISDN concepts and the structure of other I-series recommendations; I.200 deals with service aspects of ISDN; I.300 describes network aspects; I.400 describes how the User-Network Interface (UNI) is provided.
- Protocols beginning with "Q" cover how switching and signaling should operate. The term "signaling" in this context means the process of call set used. Q.921 describes the ISDN data-link processes of LAPD, which functions like Layer 2 processes in the ISO/OSI reference model. Q.931 specifies ISO/OSI reference model Layer 3 functions.

  Q.931 recommends a network layer between the terminal endpoint and the local ISDN switch. This protocol does not impose an end-to-end recommendation. The various ISDN providers and switch types can and do use various implementations of Q.931. Other switches were developed before the standards groups finalized this standard.

Q.921
↓
L2
Q.931
↓
L3

ISDN Functions/Reference Points



- **Functions are devices or hardware functions**
- **Reference points characterize different interfaces**

8

To access ISDN, you must provide functions and reference points that comply with ISDN service provider standards. By using these functions and reference points, you can improve communication with vendors and service providers while you engineer, install, and support your ISDN facilities.

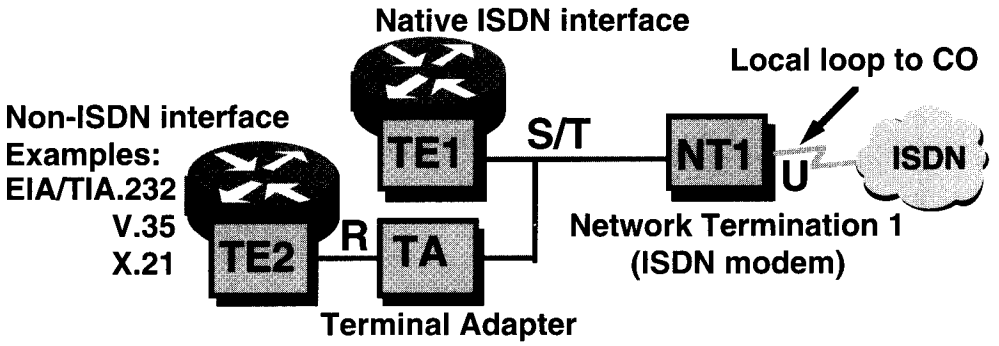
- Functions—Device types or hardware functions that represent transition points between the reference-point interfaces.

  The following table defines the basic ISDN device or hardware acronym and its function.

Acronym	Device Name	Device Function
TA	Terminal Adapter	Converts from RS-232, V.35, and other signals into BRI signals.
TE1	Terminal End-point 1	Designates a router as a device having a native ISDN interface.
TE2	Terminal End-point 2	Designates a router as a device requiring a TA for its BRI signals.
NT1	Network Termination 1	Converts BRI signals into a form used by the ISDN digital line.
LT	Local Termination	Portion of the local exchange that terminates the local loop.
ET	Exchange Termination	Portion of the exchange that communicates with other ISDN components.

- Reference points—CCITT has defined the ISDN local loop characterized by different interfaces. The standards call these key reference points R, S, T, U, and V.

Router Connections to ISDN



- **Example of a native interface—int bri 0**
- **Example of a nonnative ISDN interface—int s 0**
- **NT1 physically terminates the local loop**

9

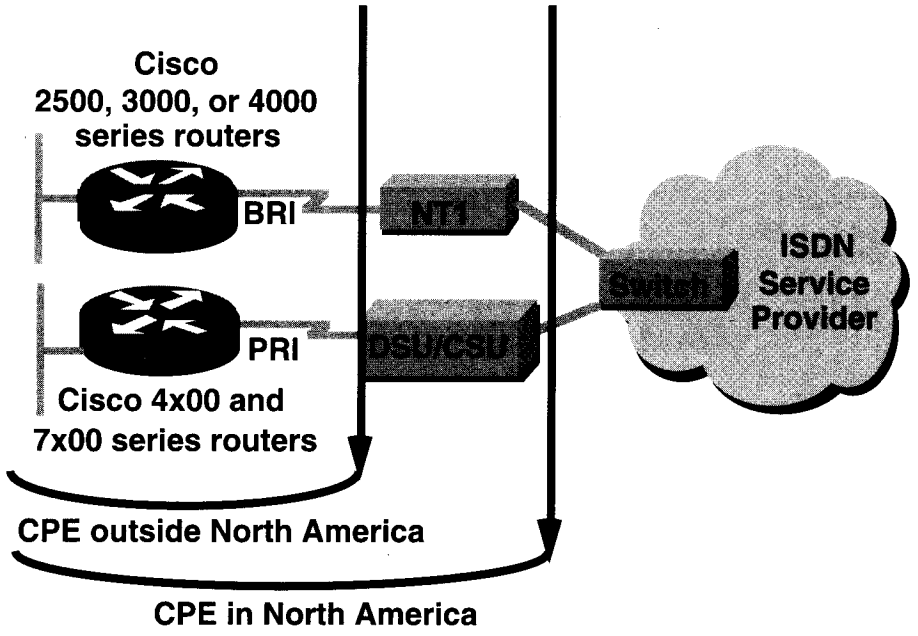
Network administrators must add one or more devices to their router to access ISDN BRI. ISDN service providers specify that these devices must perform standardized functions that they designate with two- or three-letter acronyms. To find out which ISDN devices you need to connect to ISDN, check your router.

Look on the back of your router to determine whether your router needs a TA.

- If you see a connector labeled "BRI," you already have a Basic Rate Interface. With a native ISDN interface already built-in, your router is a TE1. Your router already contains the ISDN TA function.
- If you do not see a connector labeled "BRI," your router has a nonnative ISDN interface and is a TE2. Usually this is a serial interface labeled "S0." You need to obtain an external TA device and attach it to the serial interface to provide a BRI interface.

In either case, you must obtain an external NT1. An NT1 terminates the local loop of wires to the CO of your ISDN provider. Work with your service provider to determine exactly what you need and where to obtain it.

Customer Premises to ISDN



10

ISDN specifies two main interface types: BRI and PRI.

- BRI—Two 64-kbps bearer channels (2B) plus one 16-kbps data channel (+D) service. BRI operates with Cisco 1000, 2500, 3000, and 4000 series routers. BRI connects to an NT1 for 4-wire connection.
- PRI—In North America and Japan, 23 bearer (B) channels and one 64-kbps D channel (a T1/DS1 facility).

  In Europe and much of the rest of the world, PRI offers 30 B channels and a D channel (an E1 facility). PRI uses a data service unit/channel service unit (DSU/CSU) for T1/E1 connection.

The boundary between customer premise equipment (CPE) and equipment controlled exclusively by the ISDN service provider affects hardware acquisition and operation duties required for ISDN service.

Regional differences determine who provides key ISDN functions and where the equipment is located:

- In North America and Japan, the PRI interfaces to a DSU/CSU are provisioned by the end user.
- In Europe and much of the rest of the world, the DSU/CSU is part of the ISDN service provider's equipment.

Cisco ISDN Features

- **Multiprotocol support**
- **Available on several router series**
- **SNMP support with ISDN MIB Group**
- **Multiple bearer channels**
- **Bandwidth on demand**
- **Optional incoming call screening**
- **PPP with compression options**
- **Services only when needed by using DDR**

11

As you saw earlier, ISDN provides WAN transport for all major routing protocols. ISDN also works with other WAN services such as X.25 and Frame Relay.

Cisco offers a broad range of ISDN products, including several router models that contain native ISDN interfaces. Administrators can use an SNMP-based network management application to control the ISDN interfaces. Routers use an ISDN Management Information Base (MIB) and can act as managed objects.

The multiple, independent B channels on router ISDN configurations transmit data at the standard 64-kbps (DS0) rate, or you can configure for 56-kbps facilities.

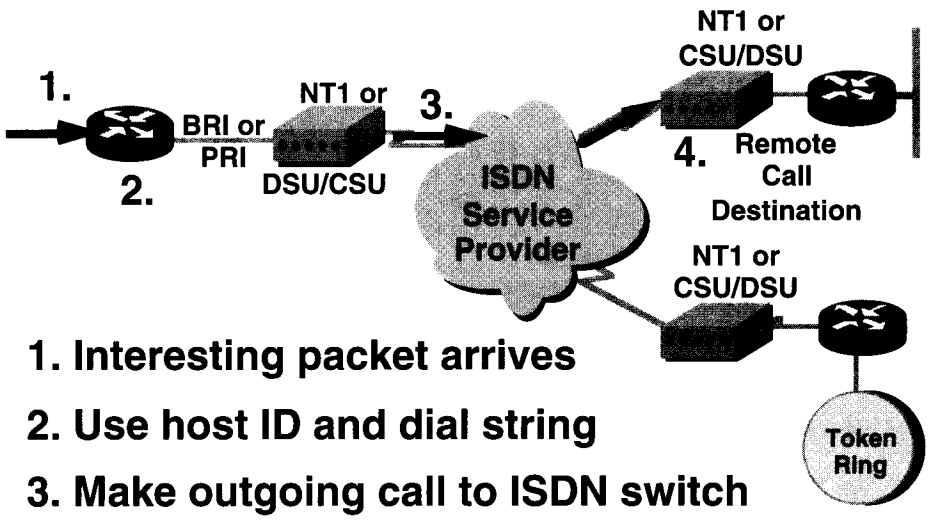
The bandwidth-on-demand option allows a preestablished load threshold setting to add available B-channel resources to an ISDN call. This DDR dialer load condition could, for example, add a DS0 on demand.

Another option on Cisco routers is to preestablish table entries on a destination router to provide incoming ISDN call screening. The destination (or called router) acts on entries that specify which calls from a source (or calling) router the destination will accept.

PPP encapsulation offers improved capabilities for standards-based access to the Internet. Among these improvements are access control and compression methods.

DDR improves the cost-effective use of ISDN by setting conditions that make the ISDN call, then dropping the call once the link is no longer needed.

Dial-on-Demand Routing for ISDN



1. Interesting packet arrives
2. Use host ID and dial string
3. Make outgoing call to ISDN switch
4. Access circuit-switched destination

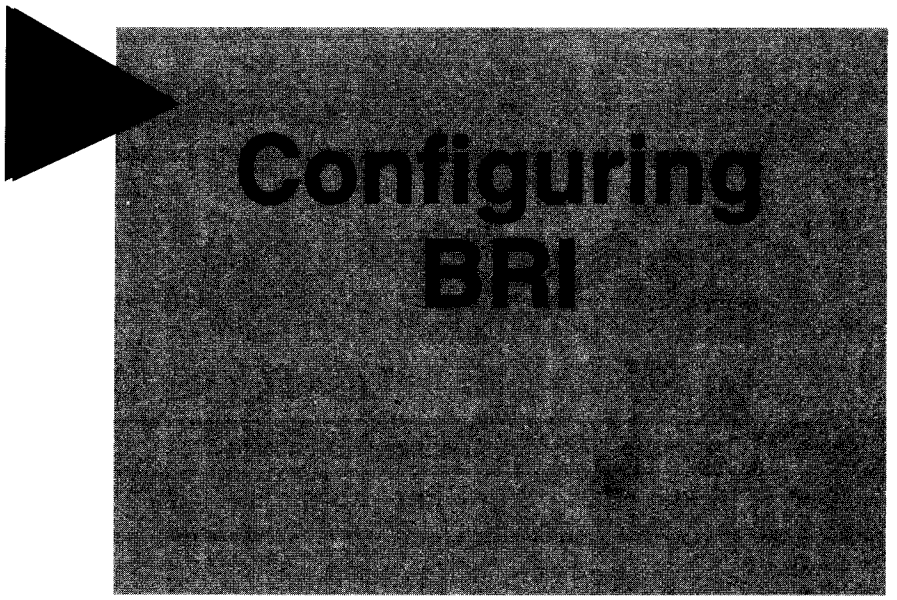
12

ISDN operates with DDR.You identify a BRI in a DDR access group and specify the protocol list (or access list) statements to check for "interesting" traffic. You can use different list settings to designate interesting traffic mapped for other DDR destination routers.

For this periodic-use environment, specify static routes so that routing updates that can be billable from the service provider are not exchanged across the ISDN cloud.

DDR commands map a host ID and dialer string to initiate setup of an ISDN call for interesting traffic. The router then makes an outgoing call from its BRI through the ISDN NT1. If using an external TA, it must support V.25 bis dialing. Calling details for these devices come from dialer commands.

ISDN end stations now use this static route to transmit packet traffic. When no more traffic is transmitted over the ISDN call, an idle timer starts. After the idle timeout occurs, the call disconnects.

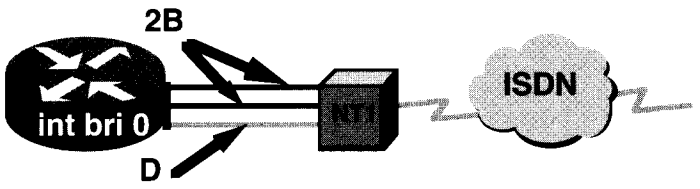


13

Configuring BRI

ISDN Channels for BRI Are 2B+D

Channel	Capacity	Mostly Used for:
B	64 kbps	Circuit-switched data (HDLC, PPP)



Channel	Capacity	Mostly Used for:
D	16 kbps	Signaling information (LAPD)

- **BRI is used globally for ISDN services**

14

BRI is sometimes written as 2B+D. This interface provides two bearer channels at 64 kbps and an additional 16 kbps signaling channel.

The B channels can be used for digitized speech transmission or for relatively high-speed data transport. Narrowband ISDN is circuit-switching oriented. The B channel is the elemental circuit switching unit.

The D channel carries signaling information (call setup) to control calls on B channels at the user-network interface. In addition to carrying signaling information, the D channel is used to carry subscriber low-rate packet data, such as alarm systems. Cisco routers do not currently use this facility. Traffic over the D channel employs the LAPD data-link-level protocol. LAPD is based on HDLC.

The call setup follows the ITU-T Q.931 recommendation for call control standards.

ISDN Configuration Tasks

- **Global configuration**
  - **Select switch type**
  - **Specify traffic to trigger DDR call**
- **Interface configuration**
  - **Select interface specifications**
  - **Configure ISDN addressing**
- **Optional feature configuration**

15

You must specify global and interface parameters to prepare the router for operation in an ISDN environment. The graphic outlines high-level tasks used for both BRI and PRI configuration. Later in this chapter, syntax and specific examples show the configuration differences for these two interfaces.

Global tasks—Select the switch that matches the ISDN provider's switch at the CO. This requirement is necessary because, despite standards, signaling specifics differ regionally and nationally. Set destination details. Indicate static routes from the router to other ISDN destinations. Establish the criteria for interesting packets in the router that initiate an ISDN call to the appropriate destination.

Interface tasks:

- Select interface specifications. Specify the interface type BRI and the number for this ISDN BRI port. For PRI, the interface task description occurs later in this chapter. The interface uses an IP address and subnet mask.
- Configure ISDN addressing with DDR dialer information and any ID supplied by the ISDN service provider. Indicate the interface is part of the dialer group using the interesting packets set globally. Additional commands place the ISDN call to the appropriate destination.

Following interface configuration, you can define optional features including time to wait for the ISDN carrier to respond to the call and seconds of idle time before the router times out and drops the call.

Selecting the ISDN Switch Type

Router (config) #

isdn switch-type *switch-type*

- **Specifies the type of ISDN switch with which the router communicates**
- **Other line configuration requirements vary for specific providers**

16

Use the **isdn switch-type** global command to specify the CO switch to which the router connects. For BRI ISDN service, the switch type can be one of the following:

Switch Type	Description
basic-5ess	AT&T basic rate switches (USA)
basic-dms100	NT DMS-100 (North America)
basic-ni1	National ISDN-1 (North America)
basic-1tr6	German 1TR6 ISDN switches
basic-nwnet3	Norwegian Net3 switches
basic-nznet3	New Zealand Net3 switches
basic-ts013	Australian TS013 switches
basic-net3	Switch type for NET3 in United Kingdom and Europe
ntt	NTT ISDN switch (Japan)
vn3	French VN3 ISDN switches
none	No specific switch specified

Specifying Traffic to Trigger Call

Router (config) #

dialer-list *dialer-group* protocol *protocol-name* [permit | deny]

Router (config-if) #

dialer-group *group-number*

Router (config-if) #

dialer map *protocol next-hop-address* name [*name*] speed *speed dial-string broadcast*

17

These commands are used to configure dial-on-demand calls that will initiate a connection. They are a review from the previous chapter, which discussed dial-on-demand routing.

Selecting Interface Specifications

Router (config) #

interface bri *interface-number*

- **Selects the interface for ISDN BRI operation**

Router (config-if) #

encapsulation [*ppp* | *hdlc*]

- **Selects framing for ISDN BRI**

18

The **interface bri** *interface-number* command designates the interface used for ISDN on a router acting as a TE1.

If the router does not have a native BRI (is a TE2 device), it must use an external ISDN terminal adapter. On a TE2 router, use the command **interface serial** *interface-number.*

Use the **encapsulation ppp** command if you want PPP encapsulation for your ISDN interface. This is the case if you want any of the rich LCP options that PPP offers (for example, CHAP authentication). You must use PPP PAP or CHAP if you will receive calls from more than one dial-up source.

To revert from PPP encapsulation to the default, use the **encapsulation hdlc** command.

Setting SPIDs if Necessary

Router (config-if) #

isdn spid1 ***spid-number*** [***ldn***]

- **Sets a B channel Service Profile Identifier (SPID) required by many service providers**

Router (config-if) #

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

- **Sets a SPID for the second B channel**

19

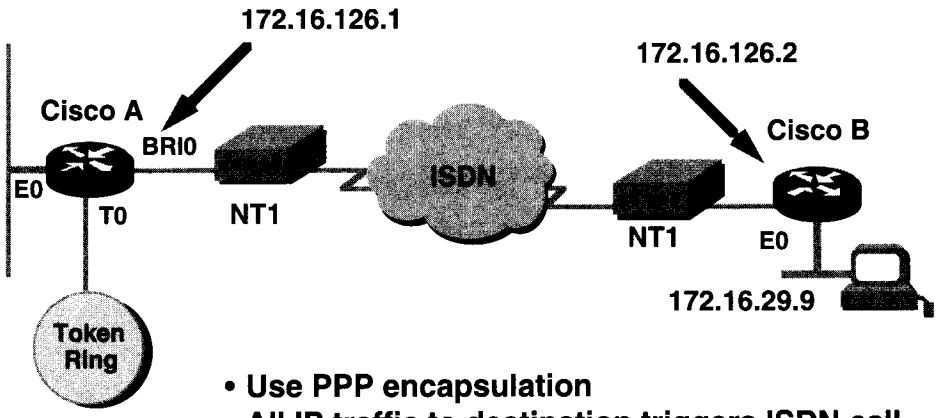
Several ISDN providers use ISDN switches that operate on dialin numbers called Service Profile Identifiers (SPIDs). These switches include National ISDN1 and DMS-100 ISDN switches, as well as the AT&T 5ESS multipoint switch.

The local SPID number is supplied by the service provider.

Use the **isdn spid1** and **isdn spid2** commands to access the ISDN network when your router makes its call to the local ISDN exchange.

isdn spid1 and **isdn spid2** Command	**Description**
spid-number	Number identifying the service to which you have subscribed. This value is assigned by the ISDN service provider.
ldn	(Optional) local dial number. This number must match the called-party information coming in from the ISDN switch in order to use both B channels on most switches.

Configuring for a Simple ISDN Call



- **Use PPP encapsulation**
- **All IP traffic to destination triggers ISDN call**
- **Carrier uses AT&T basic rate switch**
- **Service provider assigns connection parameters**

20

Here is an example of how you can combine the commands described on the previous pages to set up DDR and ISDN.

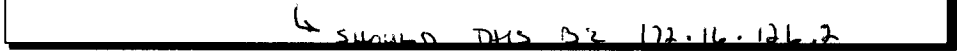
DDR is configured to connect Cisco A to Cisco B. The network between the serial interfaces of the two routers uses 8 bits of subnetting. Static route statements define the IP route to the Cisco B LAN interfaces over 172.16.126.0.

IP packets will initiate a call, but not IGRP routing updates. Interesting traffic to DDR must be defined in an access list.

The number dialed is for the remote ISDN device. This number is provided by the Regional Bell Operating Company (RBOC) offering the ISDN service. Cisco B (the next-hop router to the destination networks) has subnets 126 and 29 directly connected.

BRI Simple Configuration Example

```
! set up switch type, static route and dialer for ISDN on Cisco A
isdn switch-type basic-5ess
ip route 172.16.29.0 255.255.255.0 172.16.126.2
dialer-list 1 protocol ip permit
!
! configure BRI interface for PPP; set address and mask
interface bri 0
encapsulation ppp
ip address 172.16.126.1 255.255.255.0
!
! refer to protocols in dialer-list to identify interesting packets
dialer-group 1
!
! select call start, stop, and other ISDN provider details
dialer wait-for-carrier-time 15
dialer idle-timeout 300
isdn spid1 0145678912
! call setup details for router
dialer map ip 172.16.126.2 name cisco-b 445
```



21

In the example:

Command	Description
isdn switch-type	Selects the AT&T switch as the CO ISDN switch on this interface.
dialer-list 1 protocol ip permit	Associates permitted IP traffic with the dialer group 1. The router will not start an ISDN call for any other packet traffic with dialer group 1.
interface bri 0	Selects the interface with TA and other ISDN functions on the router.
encapsulation ppp	Use PPP encapsulation on the selected interface.
dialer-group 1	Associates the serial 0 interface with dialing access group 1.
dialer wait-for-carrier-time	Specifies a 15-second maximum time for the provider to respond once the call initiates.
dialer idle-timeout 10000	Number of seconds of idle time before the router drops the ISDN call. Note that a long duration is configured to delay termination.

dialer map Command	Description
ip	Name of protocol.
172.16.126.2	Destination address.
name	An identification for the remote side router. Refers to called router.
445	ISDN connection number used to reach this DDR destination.

Monitoring PPP on BRI

```
#sho int bri 0 1
BRI0: B-Channel 1 is up, line protocol is up
  Hardware is BRI
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive not set
  lcp state = OPEN
  ncp ccp state = OPEN  ncp ipcp state = OPEN
  ncp osicp state = NOT NEGOTIATED   ncp ipxcp state = NOT NEGOTIATED
  ncp xnscp state = NOT NEGOTIATED   ncp vinescp state = NOT NEGOTIATED
  ncp deccp state = NOT NEGOTIATED   ncp bridgecp state = NOT NEGOTIATED
  ncp atalkcp state = NOT NEGOTIATED   ncp lex state = NOT NEGOTIATED
  Last input 1w4d, output 1w4d, output hang never
  Last clearing of "show interface" counters never
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    165 packets input, 9434 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    165 packets output, 9418 bytes, 0 underruns
    0 output errors, 0 collisions, 10 interface resets, 0 restarts
    48 carrier transitions
```

22

When you have configured for ISDN, you can check the interface to see evidence of your configuration as well as some of the resulting call setup details.

If your router acts as a TE1 (has a native BRI), use the command **show interface bri** to monitor the interface and the first B channel. In the example, **show interface bri 0 1**:

Command	Description
0	The interface number. The number of the BRI.
1	The first of the two BRI B channels.

The router uses PPP encapsulation. The LCP and NCP status indicate the state and protocols that PPP can transmit over the ISDN link.

Optional Interface Configuration

- **Apply extended access lists for call trigger**
- **Enable caller ID screening**
- **Select rate adaptation**
- **Establish subaddresses**
- **Specify multilink PPP**

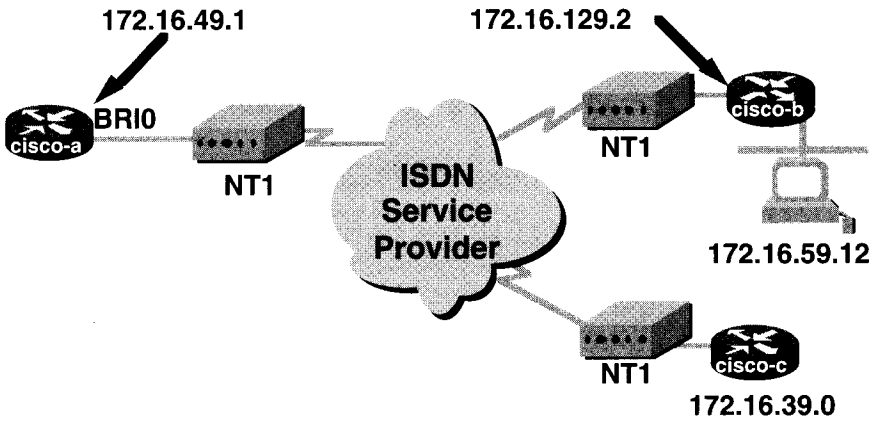
23

The first category of advanced ISDN configurations applies a more specific set of conditions for the DDR call trigger using extended access list conditions.

The second category of optional ISDN configurations applies additional interface functions desired or required by the ISDN situation:

- Use access lists for call triggers
- Filter inbound call setups with caller ID screening.
- Enable rate adaptation if calls are placed at a speed lower than 64 kbps.
- Establish subaddressing on the multipoint devices and create dialer map statements if subaddresses are required.
- Implement multilink PPP for better bandwidth use.

Extended Access List ISDN Calls



- **On cisco-a, allow all IP traffic except Telnet and IGRP to trigger ISDN call to 172.16.59.0**
- **Allow only IP traffic to all other destinations**
- **Carrier uses Northern Telecom DMS-100 switch**
- **Service provider assigns ID, timers, and dial string**

24

This example shows how you can combine commands described in the previous material on DDR to set up an extended access list to trigger an ISDN call. Use many of the same commands as you saw previously for configuring a simple ISDN call.

DDR is configured on router cisco-a to connect with cisco-b for all IP traffic except Telnet and IGRP routing updates. The details about what is interesting to DDR are defined in an access list.

The RBOC offering the ISDN service uses a Northern Telecom DMS-100 switch, so the configuration uses SPIDs. The service provider provides other details you must use when you configure your router for ISDN.

BRI Access List Example

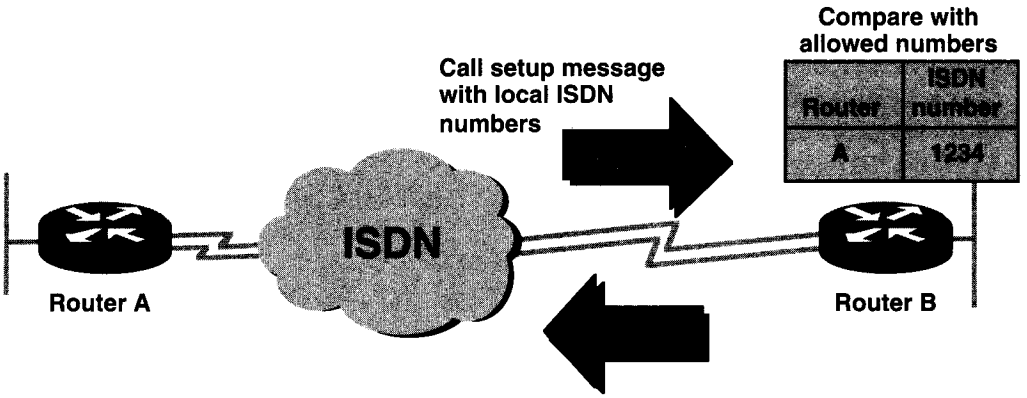
```
isdn switch-type basic-dms100
ip route 172.16.59.0 255.255.255.0 172.16.129.2
! set up conditions for call to cisco-b: only IP but not for telnet or IGRP
access-list 101 deny tcp 172.16.49.0  0.0.0.255 172.16.59 0.0.0.255 eq 23
access-list 101 deny igrp 172.16.49.0  0.0.0.255 172.16.59 0.0.0.255
access-list 101 permit ip 172.16.49.0  0.0.0.255 0.0.0.0 255.255.255.255
dialer-list 2 list 101
!
!  interface details follow
interface bri 0
ip address 172.16.49.1 255.255.255.0
!  in group that refers to access statements in dialer-list for call trigger
dialer-group 2
dialer wait-for-carrier-time 15
dialer idle-timeout 300
isdn spid1 0246864211
isdn spid2 0246864212
!   call setup details for router and NT1
dialer map ip 172.16.129.2 name cisco-b 945
```

25

In the example:

Command	Description
access-list 101 deny...	Selects an extended IP access list with a from-address on router A (a to-address on router B). Denies the IP port number equaling 21 to arrange that Telnet packets will not trigger DDR with this configuration. In the next statement, IGRP is not allowed to trigger an ISDN call.
access-list 101 permit....	Selects the same extended IP access list with a from-address on router A (a to-address of any network). All IP traffic not denied by prior statements is permitted. Other protocol packets are implicitly denied. These other protocols will not trigger DDR calls with this configuration.
dialer-list 2 list 101	Sets up control for automatic DDR dialing. Dialing group 2 connects access list 101 conditions with the following **dialer-group** command statement.
dialer-group 2	Associates the router's interface bri 0 as an interface in the group that uses the dialer list and access list 101 statements.
isdn spid1 0246864211	Sets the service provider ID as specified by the service provider for the first B channel of the ISDN line.
isdn spid2 0246864212	Sets the SPID for the second B channel on the ISDN line.
dialer map ip 172.16.129.2 name cisco-b 945	Defines the call string 945 for permitted IP traffic to the destination on a cisco-b interface.

Caller Identification Screening



- **Extra level of call management**
- **Call not set up (and charged) until acceptance**
- **Alternative: PPP encapsulation and CHAP**

26

Calling line identification screens incoming ISDN calls. The called number supplied in the call message setup request is verified against a table of allowed numbers. This feature prevents charges for calls from unauthorized numbers.

Caller ID is only available from providers that supply "called number values" in the setup request.

Note As a preferred alternative, PPP encapsulation enables PAP or CHAP. This allows an administrator to control access to ISDN if the caller ID is not used. You must use CHAP if your router receives incoming ISDN calls from multiple destinations on the same subnet.

Configuring Call Screening

Router (config-if) #

isdn caller *number*

- **Enables caller ID screening**

Router (config-if) #

isdn answer1 [*called-party-number*]

or

Router (config-if) #

isdn answer2 [*called-party-number*]

- **Sets the number to which interface responds**

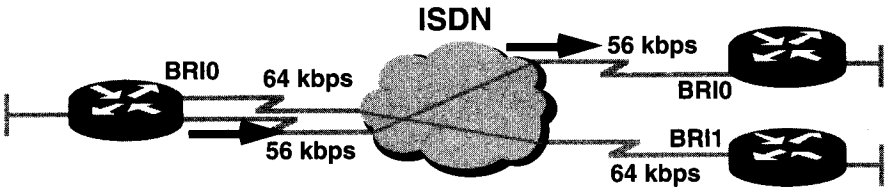
Use the **isdn caller** command to specify the numbers from which calls are accepted.

Use the **isdn answer1** or **isdn answer2** command to specify numbers to which the interface will respond in a call request. The number is the called party number, which is supplied by the ISDN network. The called party number should not be mistaken for the number used by the router to initiate the call.

isdn answer1 Command	Description
called-party-number	Number supplied in the call setup request.

Some service providers require that both **isdn answer1** and **isdn answer2** parameters be specified.

Selecting ISDN Rate Adaptation



- **Configured for outgoing calls**
- **Requested lower speed from call is honored**
- **Assigned on a per-destination basis**

28

Rate adaptation allows the ISDN channel to adjust to a lower speed if requested in the call setup. The speed may be designated in a **dialer map** statement manually configured on the router placing the call.

Use this for cases where the destination does not use the default DS0 of 64 kbps. The other alternative, used in most of North America, is 56 kbps.

Configuring Rate Adaptation

Router (config-if) #

dialer map *protocol next-hop-address* speed *speed*

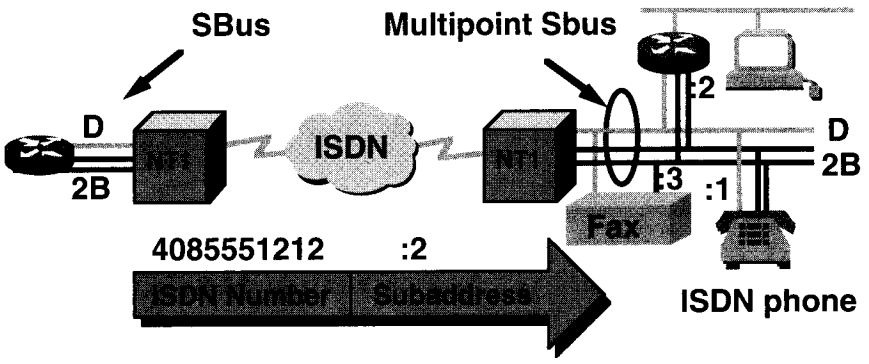
- **Negotiate speed for calls to this destination**

29

Use the **dialer map speed** command to designate the speed of a call to a remote host.

dialer map speed Command	Description
protocol	Network-layer protocol.
next-hop-address	The network-layer address of the next-hop router.
speed	The data rate can be 56 kbps or 64 kbps (the default).

ISDN SBus and Subaddresses



- **Connect NT1 to SBus with multipoint devices**
- **Specify subaddress for each multipoint device, for example, 4085551212:2**

30

The ISDN SBus (also called the S reference) allows the connection of multiple ISDN devices, creating a multipoint connection of up to eight devices accessible using the same main ISDN dial string. To sort out proper destinations, each multipoint-connected device has a unique subaddress.

There are distance limitations between the SBus equipment and the NT1 device.

ISDN subaddresses are used to connect to multipoint devices attached to the SBus. Each device on the SBus is programmed with a unique subaddress and will respond only to calls directed specifically to that subaddress.

Subaddresses are specified during the call setup request over the D channel. Subaddress service is not universally available.

Configuring Subaddresses

Router (config-if) #

dialer map *protocol next-hop-address* name *hostname dial-string* [*:isdn-subaddress*]

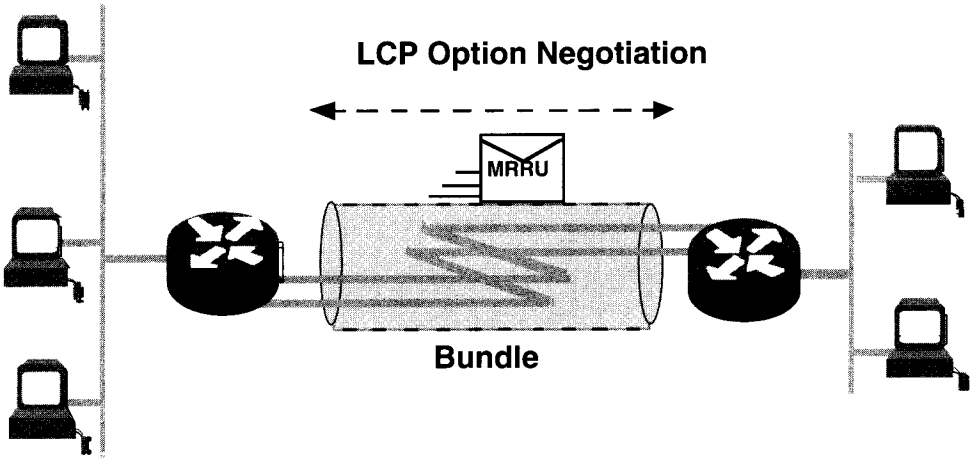
- **Specifies subaddress numbers used in ISDN multipoint connections**

Use the **dialer map protocol** command with an ISDN subaddress to specify which specific device in a multipoint destination is the target of a call.

dialer map protocol Command	Description
protocol	Protocol to be used. This can be IP, IPX, or AppleTalk.
next-hop-address	Address of the next-hop router destination.
name *hostname*	Name of the remote host used for authentication in the host name table.
dial-string	Number used to reach the remote host.
:isdn-subaddress	Subaddress of the multipoint device.

Subaddresses are not always available. An administrator should check with the ISDN provider before entering this configuration.

Multilink PPP Operation



32

Multilink PPP works over any interface that supports DDR rotary groups and PPP including ISDN, synchronous, and asynchronous interfaces.

During PPP's LCP option negotiation, a system indicates to its peer that it is willing to multilink by sending the maximum received reconstructed unit (MRRU) option as part of the initial LCP option negotiation. Multilink systems must be able to do the following:

- Combine multiple physical links into one logical bundle.
- Receive and reassemble upper-layer protocol data units (PDUs).
- Receive PDUs of a negotiated size.

After the LCP negotiation has completed, the remote destination must be authenticated and a dialer map with the remote system name must be configured. The authenticated username or caller ID is used to determine which bundle to add the link to.

Configuring Multilink PPP

Router (config-if) #

ppp multilink

- **Enables multilink on rotary group**

Router (config-if) #

dialer load-threshold *load* direction
[outbound | inbound | either]

- **Brings up links and adds them to bundle**

33

The **ppp multilink** interface configuration command enables multilink on a rotary group. The rotary group must be using PPP encapsulation.

The maximum number of links in a bundle is the number of interfaces in the dialer/ISDN interface.

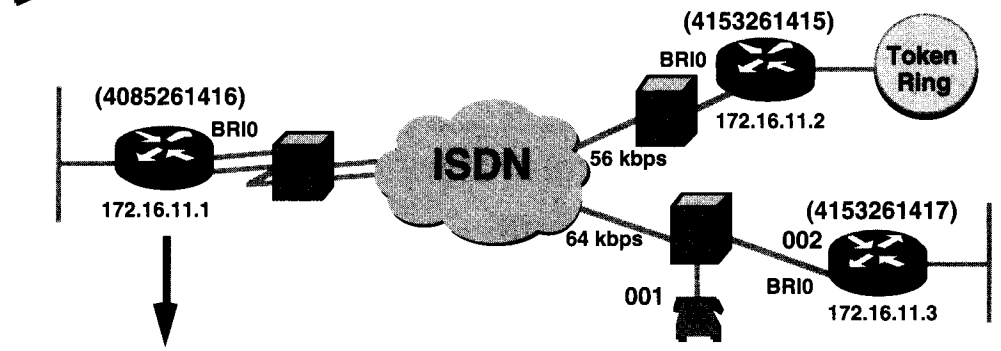
Standard DDR configuration for load balancing should be in place before configuring the multilink.

The **dialer load-threshold** command enables a rotary group to bring up links and add the links to a multilink bundle. This command has been extended to allow the threshold determination to be decided by any of the following:

- Outbound traffic only (default)
- Inbound traffic only
- The maximum of either inbound or outbound traffic

DEFAULT IS AROUND 60% PER GARY CHECK

Advanced Configuration Example




```
isdn switch-type basic-net3
interface bri 0
ip address 172.16.11.1 255.255.255.0
! accept only these calls in delivered by switch
isdn caller 4153261415
isdn caller 4153261417
dialer map ip 172.16.11.2 speed 56 4153261415
dialer map ip 172.16.11.3  4153261417:2
dialer-group 1
```

34

In the example, the switch type is one used in the United Kingdom. The configuration fields include:

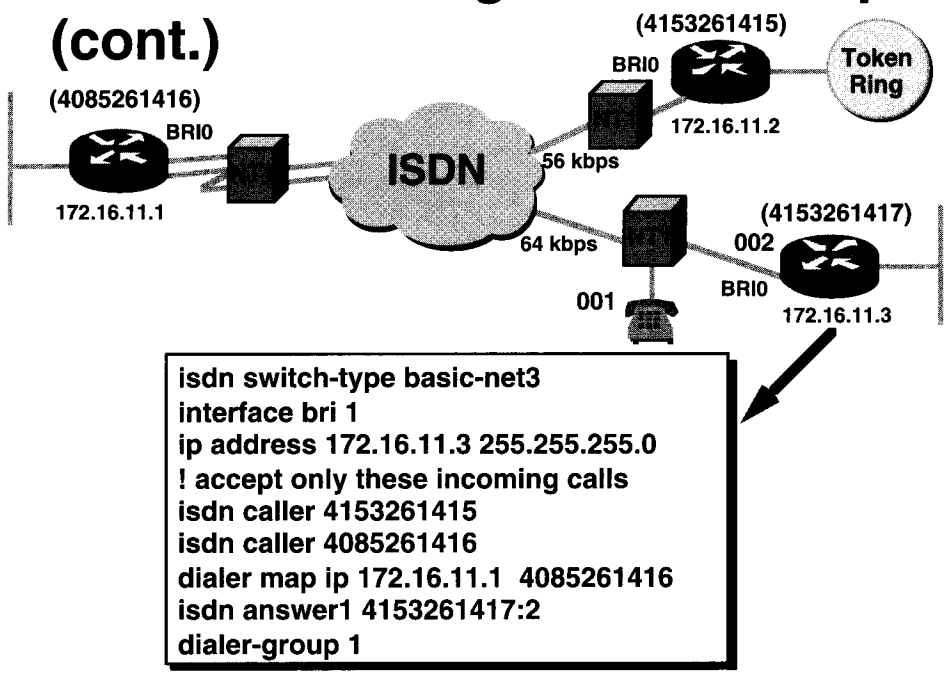
Command	Description
isdn caller 4153261415	Adds this telephone number to the table of numbers from which calls are accepted.

dialer map Command	Description
ip	Protocol.
172.16.11.2	Destination IP address.
speed 56	Sets the call setup requested speed to 56 kbps.
4153261415	The telephone number used to connect with the destination.

dialer map ip 172.16.11.3 Command	Description
4153261417:2	Number to be used to reach the destination. It contains a subaddress field :2.

The router on the left accepts calls from numbers 4153261415 and 4153261417. Calls placed to IP address 172.16.11.2 use number 4153261417, and the call setup request speed is 56 kbps.

Advanced Configuration Example (cont.)



35

On the lower right router, the configuration fields include:

Command	Description
isdn answer1 4153261417:2	Incoming calls for number 4153261417 with a subaddress of :2 are answered.

Monitoring ISDN

```
Router> show controller bri 0
BRI unit 0
D Chan Info:
Layer 1 is ACTIVATED
idb 0x32089C, ds 0x3267D8, reset_mask 0x2
buffer size 1524
RX ring with 2 entries at 0x2101600 : Rxhead 0
00 pak=0x4122E8 ds=0x412444 status=D000 pak_size=0
01 pak=0x410C20 ds=0x410D7C status=F000 pak_size=0
TX ring with 1 entries at 0x2101640:tx_count = 0,tx_head = 0,tx_tail = 0
00 pak=0x000000 ds=0x000000 status=7C00 pak_size=0
0 missed datagrams, 0 overruns, 0 bad frame addresses
0 bad datagram encapsulations, 0 memory errors
0 transmitter underruns

-- More --
```


Use the **show controller bri** command to display B- and D-channel physical-layer status information about the integrated BRI interface on a Cisco 2500, Cisco 3000, or Cisco 4000 series router.

Monitoring ISDN (cont.)

```
Router> show interface bri0 1
BRI0: 1 is up, line protocol is up
  Hardware is BRI
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive set (10 sec)
  DTR is pulsed for 1 seconds on reset
  LCP Open
  Open: IPCP
  Last input 4d10, output 4d10, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     26 packets input, 866 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     34 packets output, 1017 bytes, 0 underruns
     0 output errors, 0 collisions, 12 interface resets, 0 restarts
     8 carrier transitions
```

37

Use the **show interface bri0 1** command to display information about the B1 channel. To see information about both B1 and B2 channels, enter the **show interface bri0 1 2** command. If the command is entered without the parameters 1 and 2, only D channel status is shown.

Monitoring Multilink PPP

```
Router# show dialer
BRI0 - dialer type = ISDN
Dial String    Successes   Failures   Last called   Last status
81012345678902       2          0       0:03:02     Successful
0 incoming call(s) have been screened.
BRI0: B-Channel 1
Idle timer (30 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Time until disconnect 9 secs
Current call connected 0:03:03
Connected to 81012345678902
BRI0: B-Channel 2
Idle timer (30 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Current call connected 0:03:04
Connected to 81012345678902
Packet Muxing
Group = 81012345678902 : No. members = 2 : Rec. seq = A : Send seq = A
Group = 81012345678902 : lost packets = 0 : Out of order  = 3
Group = 81012345678902 : Unassigned = 0 : First link = BRI0: B-Channel 1
```


The **show dialer** command displays bundle information on a rotary group in the packet muxing section including:

- Number of members in a bundle
- Which bundle a link belongs to

Summary

One signaling channel and multiple data channels

ISDN has two operational modes:

- BRI on the Cisco 1000, 2500, 3000, and 4x00 series
- PRI on the Cisco 7x00 and 4x00 series

You may need an external TA; you will need an external NT1 or CSU/DSU

Set parameter values for attaching as specified for the ISDN-provider switch

Use standard DDR commands for making an ISDN call

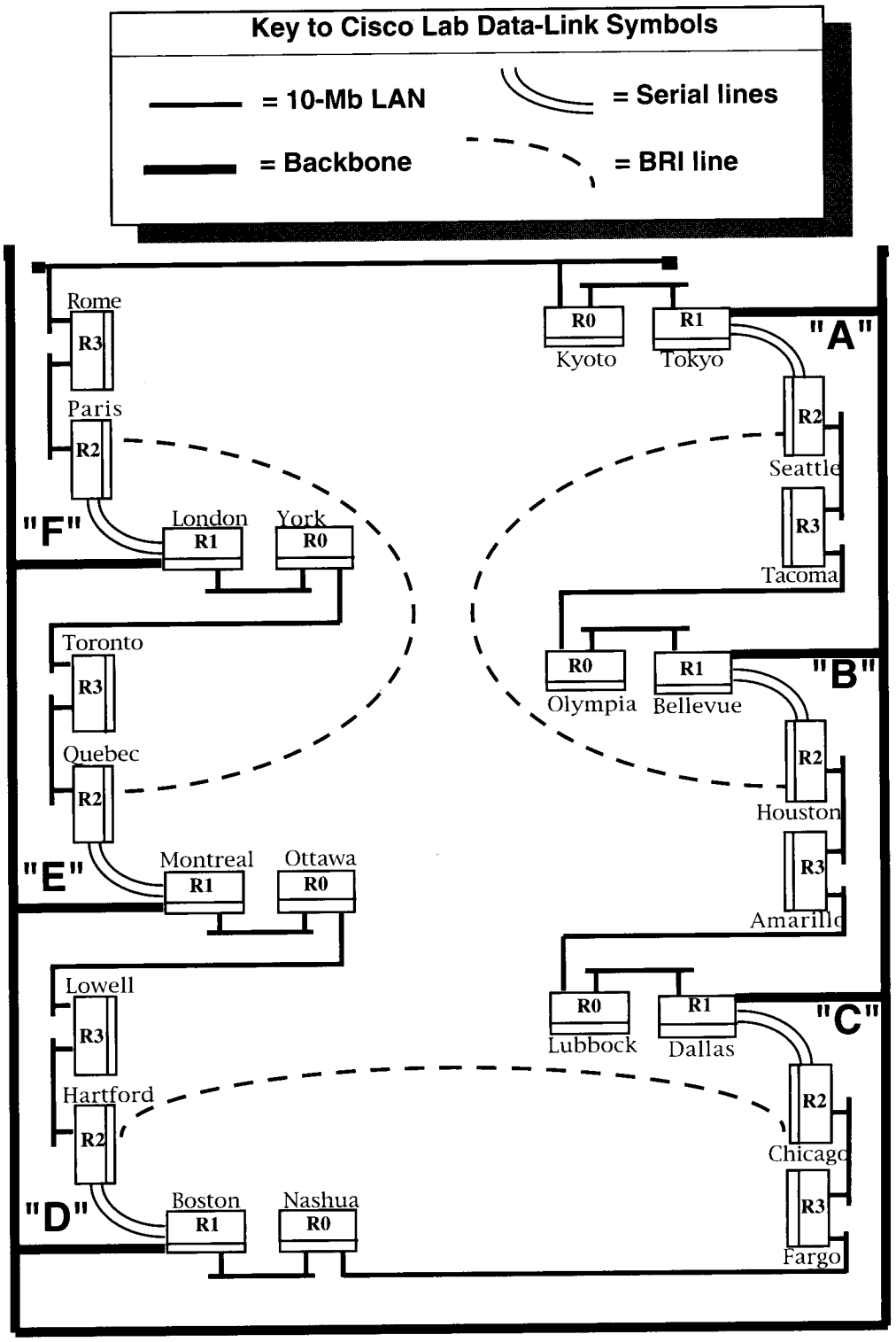
Caller ID screening provides security

Multilink PPP provides load balancing

39

Lab: ISDN Basic Rate Interface Implementation

Map of the Cisco Lab Internetwork



ISDN BRI Lab Preparation

Objective: Configure an ISDN call, open a circuit, and pass data over an interface.

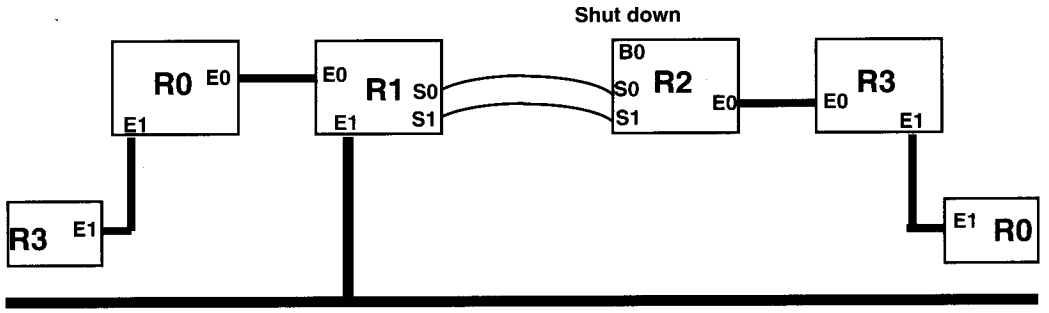
Objective: Monitor and analyze ISDN operation through the router.

Referring to the diagram of the classroom lab on the previous page, use Cisco IOS software statements to configure a BRI call. This call is for TCP/IP traffic from the routers in your group to the R2 router on another group.

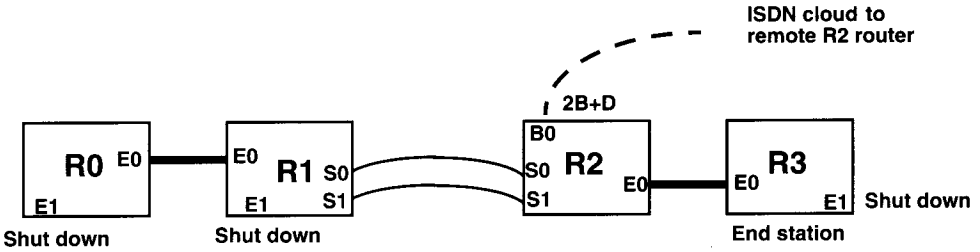
Instructions: Before you configure for the BRI connection to the other R2 router, you must first reconfigure your group interfaces to simulate a four-router remote campus. All connections beyond this campus will use ISDN BRI. R2 will be the focus for this ISDN call.

Step 1 Use the Cisco IOS software commands necessary to change your group to a configuration like the diagram labeled "Group Router Interfaces after Preparation for the WAN Labs."

Group Router Interfaces from Prior Labs



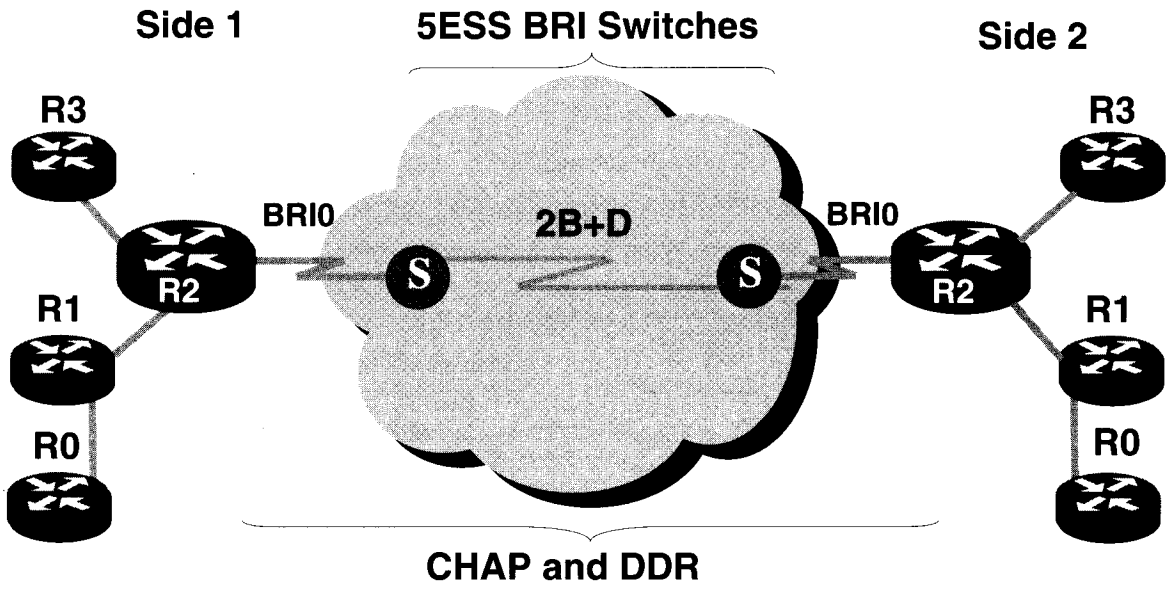
Group Router Interfaces after Preparation for the WAN Labs



Step 2 Verify that the other connections to the classroom backbone are disabled.

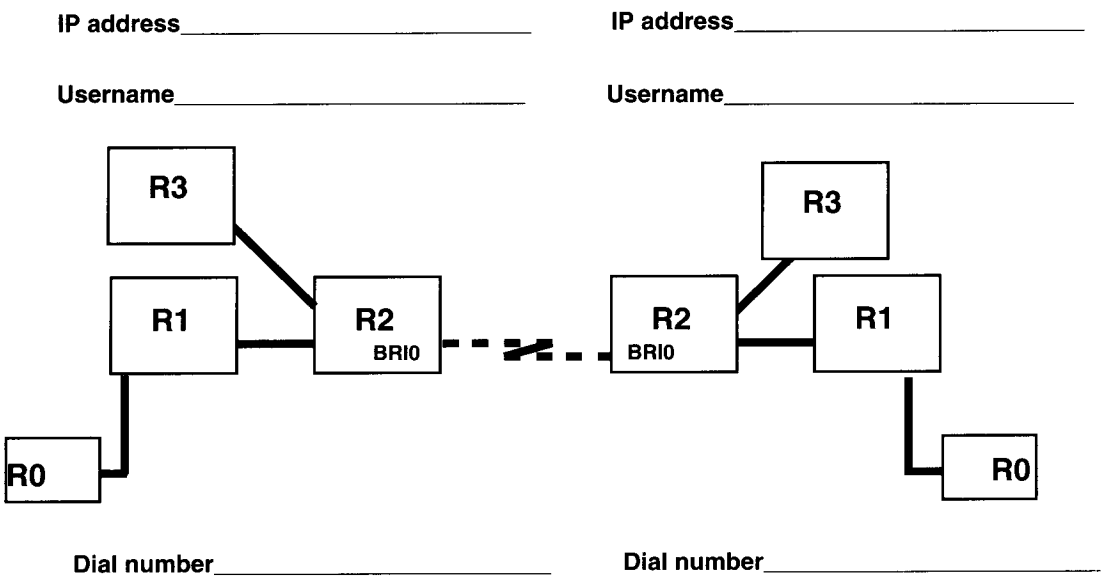
AT&T 5ESS Switch BRI Planning

On the R2 router configure the following: PPP encapsulation with CHAP; a DDR call; a static route to a destination on the remote group; and the calling information entries provided for the BRI calls to and from your group over the BRI link. Refer to the diagram.



Use the following information as you prepare to configure the R2 router:

- AT&T 5ESS switches emulated in this lab will follow the recommendation that the ISDN service not require SPIDs.
- Use PPP encapsulation with CHAP authentication.
- Use the destination city name for the CHAP username and for your dialer map destination name. Use the password *cisco*.
- As you set up for the BRI connection between the two R2 routers, the IP address for BRI0 on all side 1 R2 routers (Seattle, Chicago, and Quebec) will be 10.0.0.1.
- The IP address for BRI0 on all side 2 R2 routers (Houston, Hartford, and Paris) will be 10.0.0.2.
- You will need to add the network to the IP routing protocol used by the groups.
- Your ISDN provider specifies that side 1 R2 routers use the dial number 555-2000.
- Your ISDN provider specifies that side 2 R2 routers use the dial number 555-1000.
- Set the timeout for your call to drop after exceeding 600 seconds idle.
- To trigger the call, use a dialer list that permits the protocol IP. Use the number 1 for the dialer list you create.
- You must collaborate with the group on the other side to establish compatible configurations. On the graphic on the next page, enter the IP addresses, usernames (city names), and dial numbers that your two sides will use.



Set the CHAP password to *cisco*

Step 1 Use the **isdn switch-type** command to specify the 5ESS switch type for BRI.

Step 2 Restart the router with **reload** so that the router will load information about the ISDN switch that you specified.

Step 3 When the router comes back up, set up the global commands that CHAP will use. Use the **username** command to set the target username to the city name of the R2 router on the other group. Use the password *cisco*.

Step 4 Enter the **dialer-list 1 protocol ip permit** command so that dialer will permit all IP traffic.

Step 5 Set up the interface commands. Check that the BRI0 interface on R2 is shut. If it is not, use a config-if command to **shut** it.

Step 6 Use the **ip address** command to specify the address for the BRI interface on R2 with no subnetting.

Step 7 Use PPP encapsulation. Then specify **ppp authentication chap**.

Step 8 Set the **dialer idle-timeout** to 600 seconds.

Step 9 Use the **dialer map ip** command to map the destination IP address on the link for the destination city name to use the dial number. Indicate that broadcast traffic may cross this BRI link.

Step 10 Configure the interface with a **dialer-group** command so that the interface uses the previous dialer list statement.

Step 11 Set up the **config-router** command so that **router igrp 200** will route network 10.0.0.0.

Step 12 Enter the global command to define an **ip route** default for 0.0.0.0 with the mask 0.0.0.0 that will use a target host address on network 10.0.0.0.

Step 13 As soon as you have completed the configuration, double-check the commands with everyone in your group. Also double-check with the other group.

Step 14 Bring up the BRI interface by removing the shut.

Step 15 Send extended IP ping traffic that the R2 should use as "interesting" traffic to make the call.

Step 16 After the call successfully opens, you should see an indication of successful ping echoes.

Step 17 Monitor the status of your R2-related ISDN indicators with **show** commands.

Note After the completion of this lab, remove the dialer-list access-list statements, and shut down the BRI interface.

CHAPTER 18

Configuring X.25

Objectives

Upon completion of this chapter, you will be able to perform the following tasks:

Describe the X.25 protocol stack

Describe key features of X.25

Configure X.25 on router interfaces

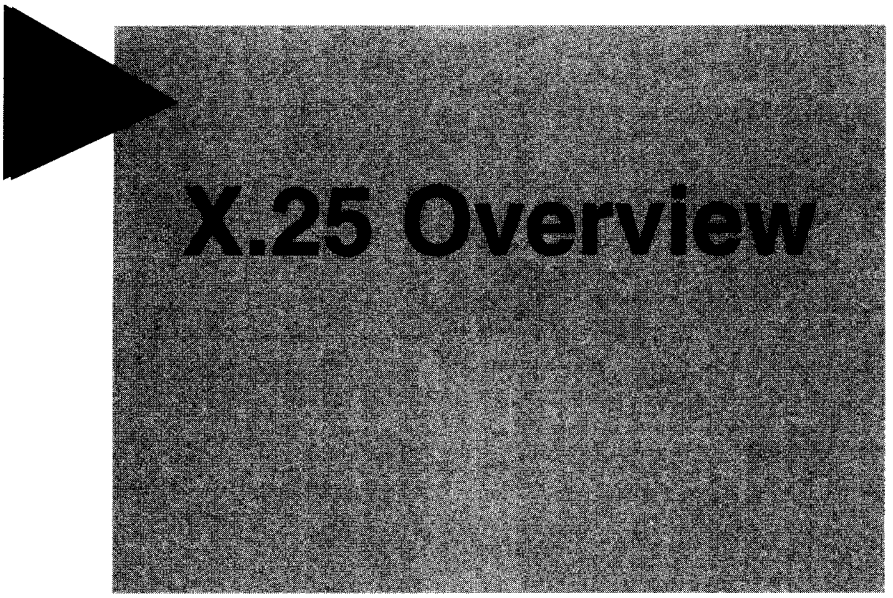
Monitor X.25 operation in the router

2

This chapter covers X.25 routing. It presents an overview of the X.25 protocol and explains how packets are addressed and encapsulated in X.25. It describes how to configure X.25 routing.

Sections:

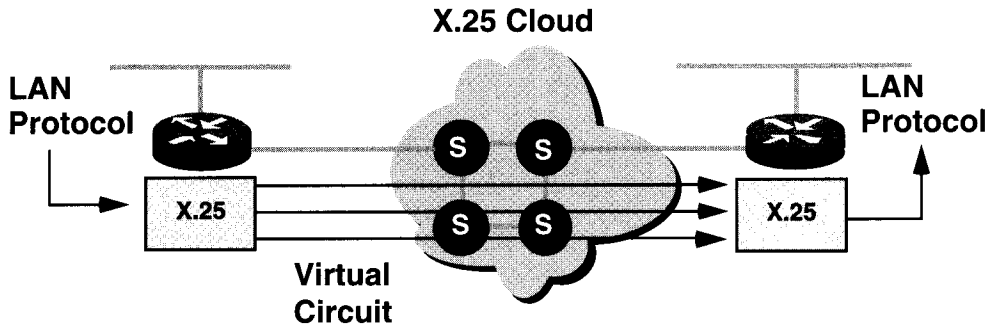
- X.25 Overview
- Configuring X.25



3

X.25 Overview

An Introduction to X.25



- IP
- AppleTalk
- Novell IPX
- Banyan VINES
- XNS
- DECnet
- ISO-CLNS
- Apollo
- Compressed TCP
- Bridging

4

X.25 is a standard that defines the connection between a terminal and a packet-switching network. X.25 offers the closest approach to worldwide data communication available. Virtually every nation uses some X.25-addressable network.

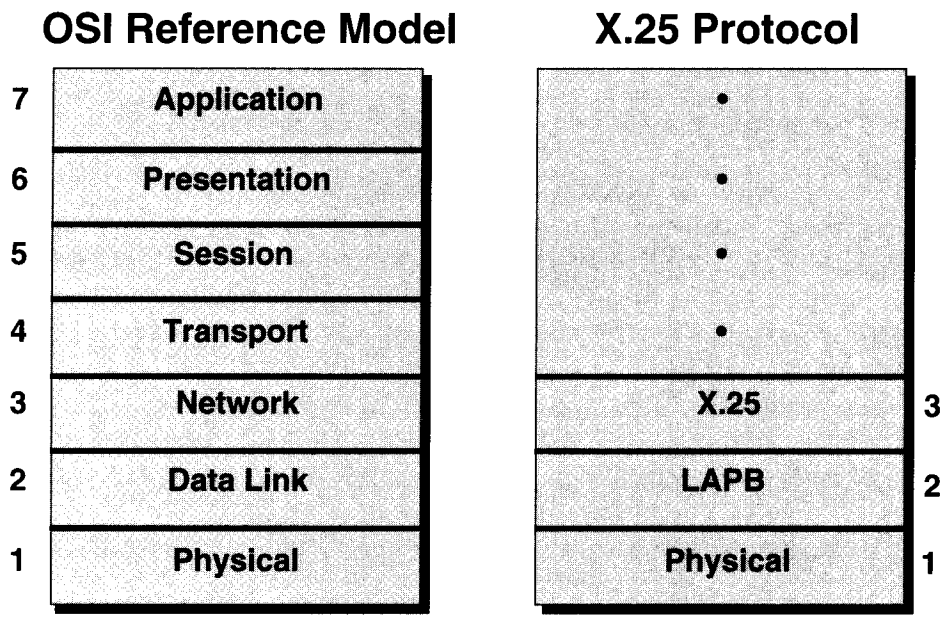
X.25 originated in the early 1970s. The networking industry commonly uses the term X.25 to refer to the entire suite of X.25 protocols.

Engineers designed X.25 to transmit and receive data between alphanumeric "dumb" terminals through analog telephone lines. X.25 enabled dumb terminals to remotely access applications on mainframes or minicomputers.

Because modern desktop applications needed LAN-to-WAN-to-LAN data communication, engineers designed newer forms of wide-area technology—Integrated Services Digital Network (ISDN) and Frame Relay (also covered in this module). In many situations, these newer WANs complement or extend, rather than replace, X.25.

Many different network-layer protocols can be transmitted across X.25 virtual circuits (VCs). This results in "tunneling" that has datagrams or other Layer 3 packets within the X.25 Layer 3 packets. Each Layer 3 packet keeps addressing legal for its respective protocol, while the X.25 VC transports the packet across the WAN.

X.25 Protocol Stack



5

The X.25 packet switching protocol suite compares to the lower three layers of the Open System Interconnection (OSI) model.

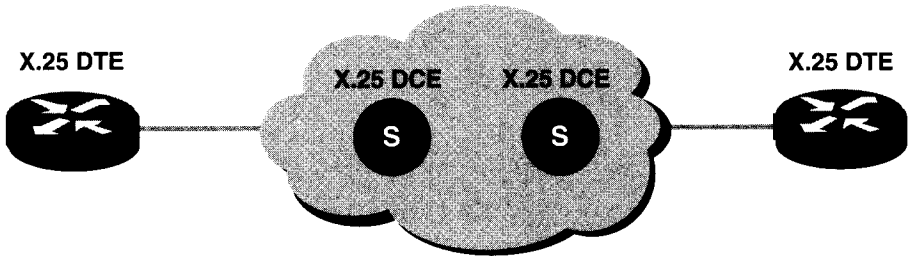
In general, we use X.25 as an overengineered data link in the internetworking world. Both X.25 at Layer 3 and Link Access Procedure, Balanced (LAPB) at Layer 2 provide reliability and sliding windows. Layers 3 and 2 were designed with strong flow control and error checking to reduce the requirement for these functions external to X.25.

X.25 evolved in the days of analog circuits when error rates were much higher than today. For analog circuit technology at Layer 1, it is more efficient to build more reliability into the network at the hardware level. With digital or fiber-optic technologies, the error rates have dropped dramatically. Newer technologies such as Frame Relay have taken advantage of this by providing a stripped-down "unreliable" data link.

X.25 was designed in the days of alphanumeric terminals and computing on central time-sharing computers. Demands on the packet switch were lower than today. Complex applications on desktop workstations demand more bandwidth and speed. Newer technologies such as ISDN and X.25 over Frame Relay add packet-switching capability.

X.25 DTE and DCE

Public Data Network (PDN)



- **X.25 DTE—Usually a subscriber's router or PAD**
- **X.25 DCE—Usually a PDN's switch or concentrator**

6

Data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for X.25 identify the responsibilities of the two stations on an X.25 attachment. The X.25 protocol implements virtual circuits between the X.25 DTE and X.25 DCE.

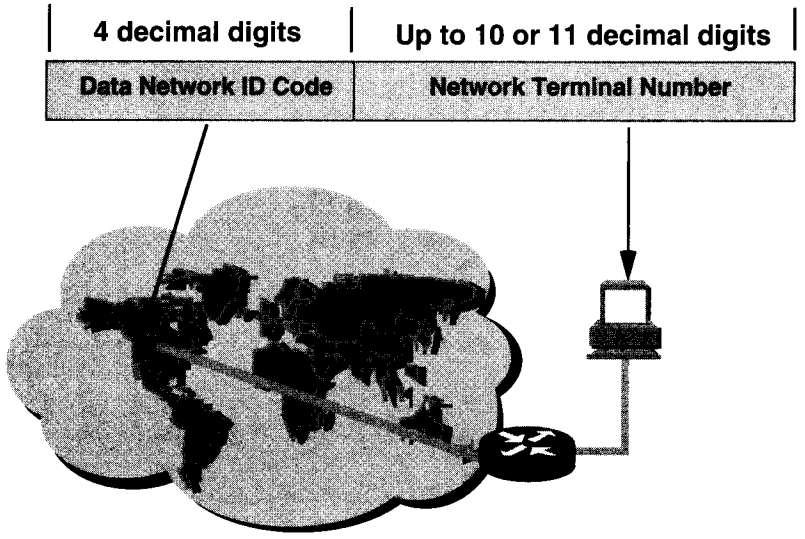
Although the terms DTE and DCE occur at all three of the layers associated with the X.25 stack, the use shown in the graphic identifies responsibilities independent of the physical-layer DTE/DCE.

The X.25 DTE is typically a router or a packet assembler/disassembler (PAD).

The X.25 packet-level DCE typically acts as a boundary function to the public data network (PDN) within a switch or concentrator. The X.25 switch at the carrier site may also be called data switching equipment (DSE). X.25's use of DTE/DCE terminology differs from the usual physical-layer interpretation.

The way X.25 traffic is carried within the carrier cloud depends on the implementation. In some cases, X.25 is also used within the cloud.

X.25 (X.121) Addressing Format



- **Addressing set by service provider**

7

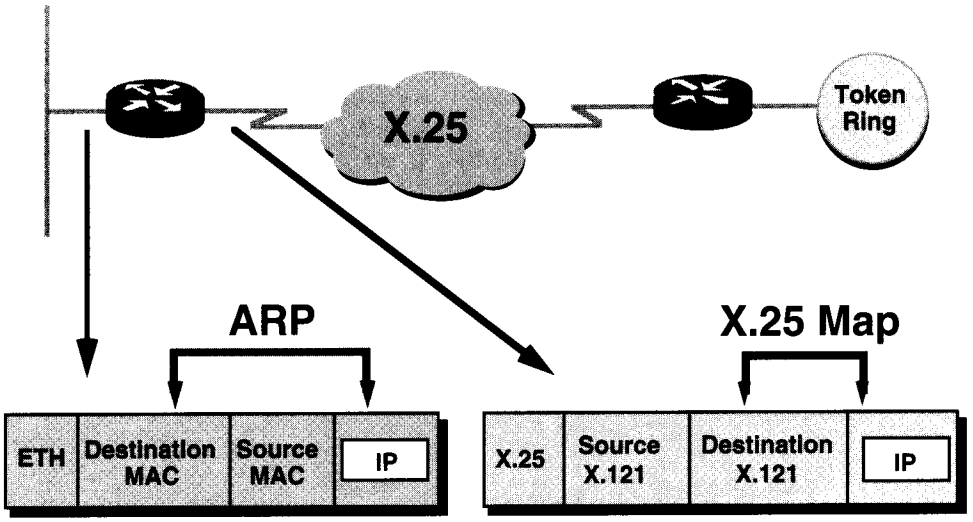
The format of X.25 addresses is defined by the ITU-T X.121 standard.

- The first four digits specify the Data Network Identification Code (DNIC). This address field is the country code and provider number assigned by the ITU.
- The remaining 8 to 10 or 11 digits specify the network terminal number (NTN) assigned by the packet-switched network (PSN) provider.

Private X.25 networks may assign addresses that best fit their network architecture.

Only decimal digits are legal for X.121 addresses. The router accepts an X.121 address with as few as 1 or as many as 15 digits. Some networks allow subscribers to use subaddresses (one or more digits after the assigned base address).

X.25 Address Resolution

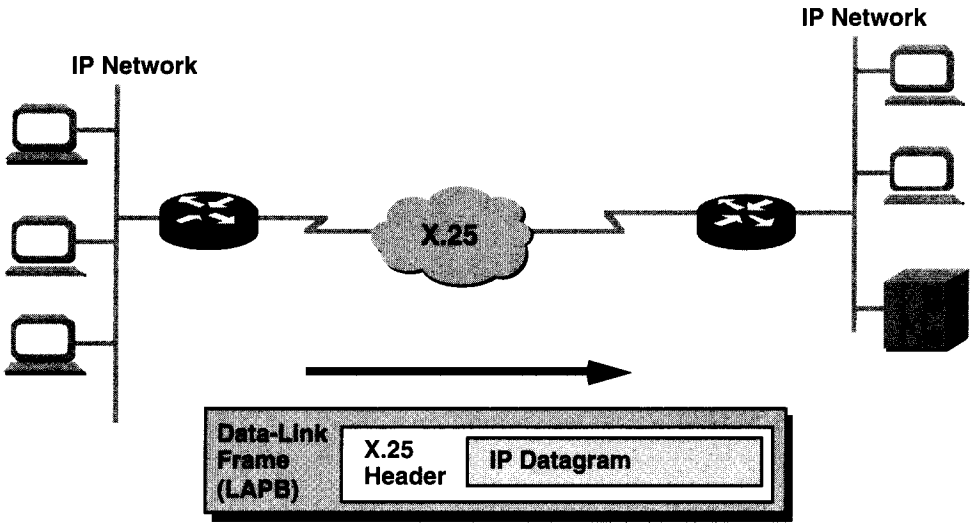


8

For different network protocols to connect across X.25, statements are entered on the router to map the next-hop network-layer address to an X.121 address. For example, an IP network-layer address is mapped to an X.121 address to identify the next-hop host on the other side of the X.25 network.

This is logically equivalent to the LAN Address Resolution Protocol (ARP) that dynamically maps a network-layer address to a data-link MAC address. Maps are required for each protocol because ARP is not supported in an X.25 network. Mapping statements are a manual configuration step required when setting up X.25 on the router.

X.25 Encapsulation



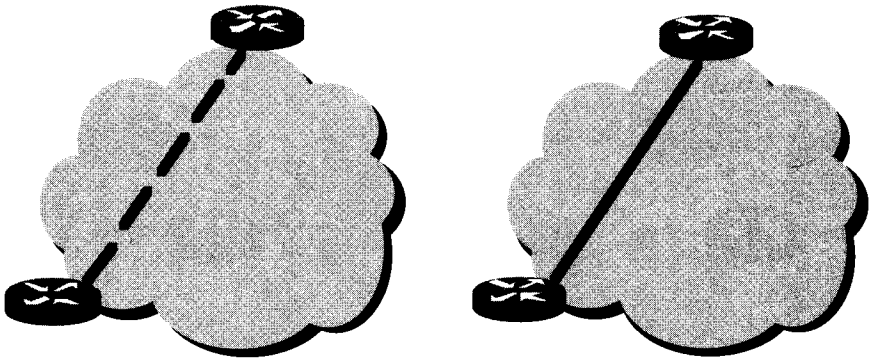
- **Protocol datagrams are reliably carried inside X.25 frames**

9

Movement of network-layer data through the internetwork usually involves encapsulation of datagrams inside media-specific frames. As each media frame arrives at the router and the media frame is discarded, the router analyzes the datagram and places it inside a new frame as it is forwarded.

Similarly, in an X.25 environment, the LAPB frame arrives at the router, which extracts the datagram from the packet or packets. The router discards the encapsulating frame and analyzes the datagram to identify the format and next hop. Based on the route determination, the router reencapsulates the datagram in framing suitable for the outgoing media as it forwards the traffic.

X.25 Virtual Circuits



Switched Virtual Circuits (SVCs)

Permanent Virtual Circuits (PVCs)

- **Numbering for up to 4095 VCs per X.25 interface**

10

VCs are used interchangeably with the terms virtual circuit number (VCN), logical channel number (LCN), and virtual channel identifier (VCI).

A VC can be a permanent virtual circuit (PVC) or, more commonly, a switched virtual circuit (SVC). An SVC exists only for the duration of the session.

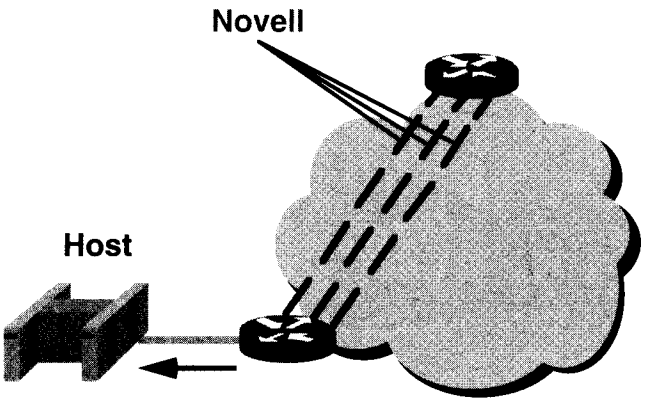
There are three phases associated with SVCs:

- Call setup
- Information transfer
- Call clear

A PVC is similar to a leased line. Both the network provider and the attached X.25 subscriber must provision the virtual circuit. PVCs use no call setup or call clear that is apparent to the subscriber. Any provisioned PVCs are always present, even when no data traffic is being transferred.

The X.25 protocol offers simultaneous service to many hosts (for example, multiplex connection service). An X.25 network can support any legal configuration of SVCs and PVCs over the same physical circuit attached to the X.25 interface. However, configuring a large number of VCs over a serial interface may result in poor performance. X.25's original design aim assumed service for time-sharing and terminal-to-host applications, not contemporary computer-to-computer applications.

SVC Usage



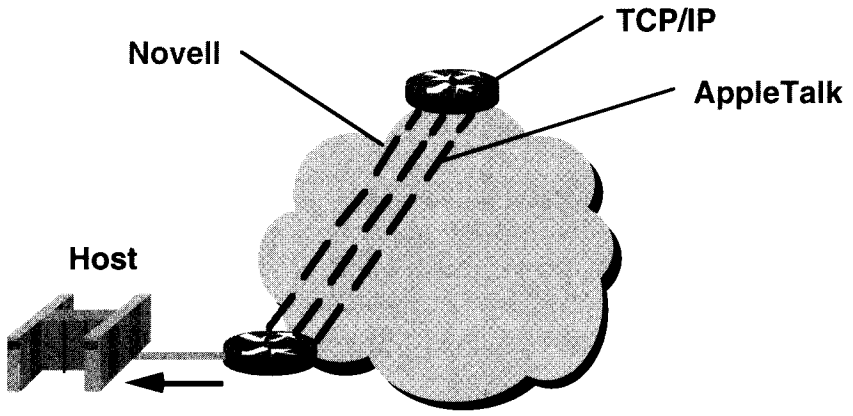
- **SVCs may be combined to improve throughput for a particular protocol**
- **A maximum of eight SVCs per protocol per destination is allowed**

11

Throughput for encapsulating a specific protocol can be improved using multiple SVCs. Multiple SVCs provide a larger effective window size, especially for protocols that offer their own higher-layer resequencing.

This combination of SVCs does not benefit traditional X.25 applications such as those available from a time-sharing host.

Single Protocol Virtual Circuits



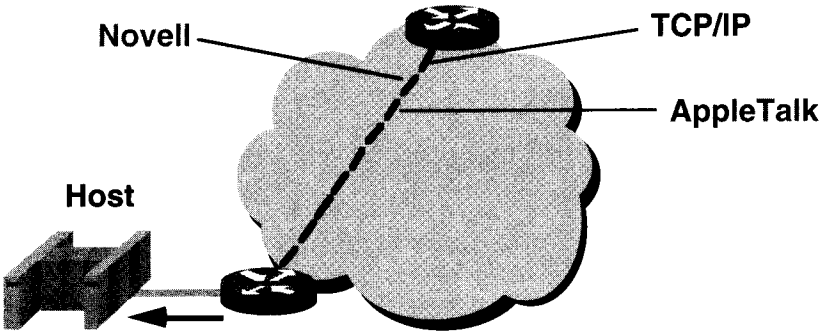
- **Each network-layer protocol is associated with its own virtual circuit**

12

The Cisco router's traditional encapsulation method enables different protocols to transport their datagrams through an X.25 cloud because the router uses separate virtual circuits.

Each protocol is specified in an individual **x25 map** command statement that references the X.121 address used to reach the destination.

Multiprotocol Virtual Circuits

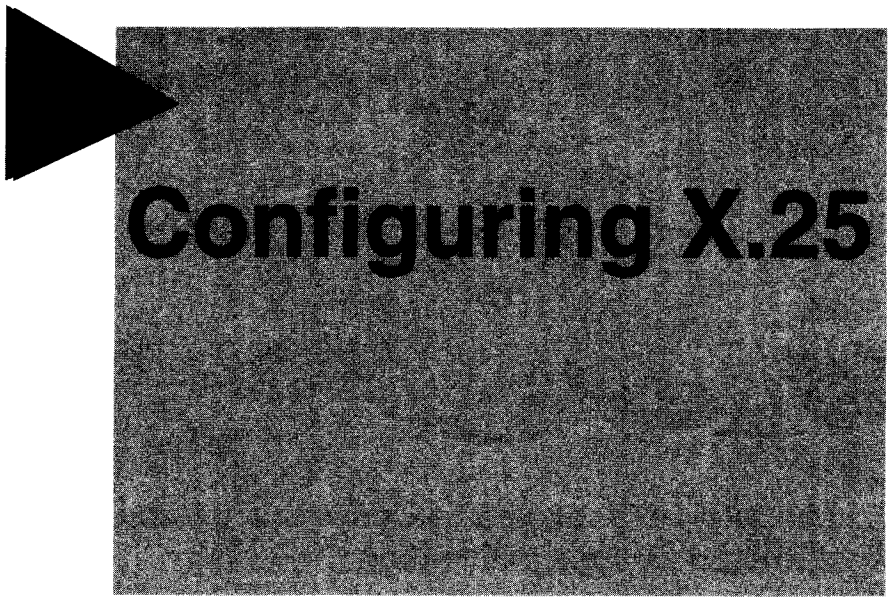


- **Multiple protocols are carried within a virtual circuit to a single destination**
- **A maximum of nine protocols may be mapped to a host**

13

In Cisco IOS Release 10.2 and later releases, a single virtual circuit to a host can carry traffic from multiple protocols. One X.25 map statement contains several protocol addresses mapped to a single X.121 address associated with the destination host.

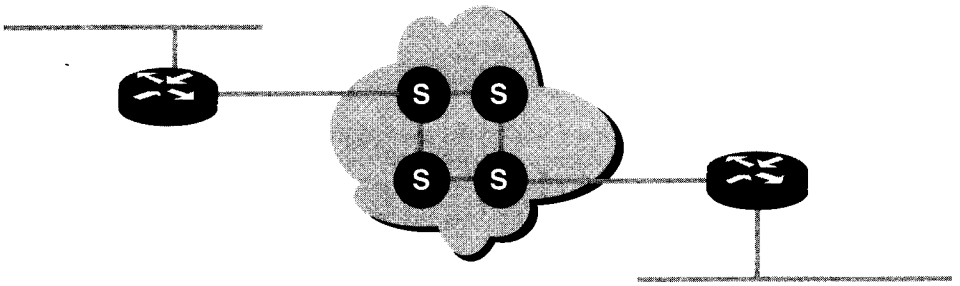
This capability uses the method described in RFC 1356. Each of the supported protocols can map to a destination host. Because higher traffic loads are generated by routing multiple protocols over a VC, combining SVCs as described earlier in this chapter may improve throughput.



14

Configuring X.25

X.25 Configuration Tasks



Interface configuration

— Select X.25 DTE or DCE encapsulation

— Configure parameters for X.25 network attachment

— Map protocol address to X.121 address

— Additional configuration steps

15

When you select X.25 as a WAN protocol, you must set appropriate interface parameters.

Interface tasks:

- Define the X.25 encapsulation (DTE is the default).
- Assign the X.121 address (usually supplied by the PDN service provider).
- Define map statements to associate X.121 addresses with higher-level protocol addresses.

Other configuration tasks can be performed to control data throughput and to ensure compatibility with the X.25 network service provider. Commonly used parameters include the number of VCs allowed and packet size negotiation.

X.25 is a flow-controlled protocol. The default flow-control parameters must match on both sides of a link. Mismatches because of inconsistent configurations can cause severe internetworking problems.

X.25 Configuration

Router (config-if) #

encapsulation x25

Router (config-if) #

encapsulation x25 dce

- **Defines encapsulation type**

Router (config-if) #

x25 address *x.121-address*

- **Establishes interface address**

16

Use the **encapsulation x25** command to specify the encapsulation style to be used on the serial interface.

The router can be an X.25 DTE, which is typically used when the X.25 PDN is used to transport various protocols, or the router can also be configured as an X.25 DCE, which is typically used when the router acts as an X.25 switch.

The **x25 address** command defines the local router's X.121 address (one address per interface). The value specified must match the address designated by the X.25 PDN.

X.25 Configuration (cont.)

Router (config-if) #

x25 map *protocol address x.121-address* [*options*]

- **Specifies how a single protocol reaches a destination**

Router (config-if) #

x25 map *protocol address* [*protocol2 address2*]* *x.121-address* [*options*]

- **Specifies how multiple protocols reach a single destination using one SVC**

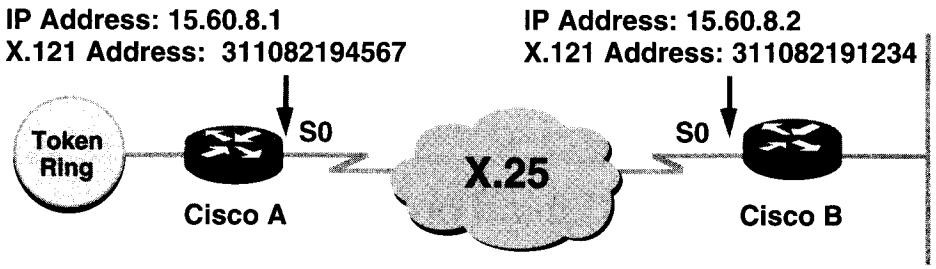
17

The **x25 map** command provides a static conversion of higher-level addresses to X.25 addresses. The command correlates the network-layer addresses of the peer host to the peer host's X.121 address.

x25 map Command	Description
protocol	Selects the protocol type. Supported protocols are: ip, xns, decnet, ipx, appletalk, vines, apollo, bridge, clns, and compressed tcp.
address	Specifies the protocol address (not specified for bridged or CLNS connections).
x.121-address	Specifies the X.121 address. Both the protocol address and the X.121 addresses are required to specify the complete network protocol-to-X.121 mapping.
options	(Optional) Used to customize the connection.

Use the second **x25 map** statement only when trying to communicate with a host that understands multiple protocols over a single VC. This communication requires the multiprotocol encapsulations defined by RFC 1356. In the second **x25 map** command, the "*" means that a maximum of nine network protocol addresses may be associated with one host destination in a single configuration command. Bridging is not supported.

X.25 Configuration Example



Cisco A

```
interface serial 0
encapsulation x25
x25 address 311082194567
ip address 15.60.8.1 255.255.248.0
x25 map ip 15.60.8.2  311082191234
```

Cisco B

```
interface serial 0
encapsulation x25
x25 address 311082191234
ip address 15.60.8.2 255.255.248.0
x25 map ip 15.60.8.1  311082194567
```

18

In the example:

Command	Description
encapsulation x25	Sets the encapsulation style on interface serial 0 to X.25 type.
x25 address 311082194567	Establishes the X.121 address of serial 0.

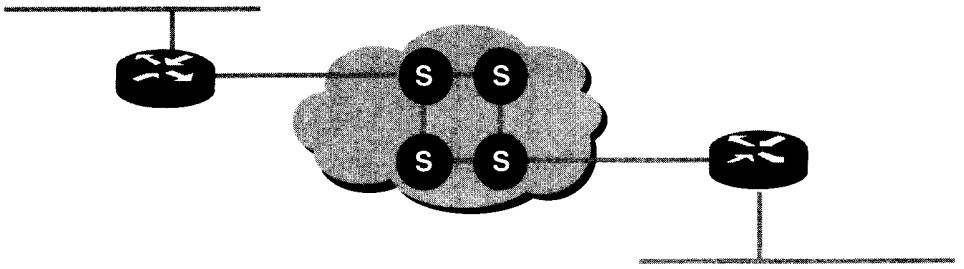
x25 map Command	Description
ip	A Layer 3 protocol specified for address association.
15.60.8.2	IP address that is mapped.
311082191234	The X.121 address of the host that defines the IP address.

IP routing on Cisco A forwards datagrams destined for subnet 15.60.8.0 to interface serial 0. The interface map identifies the destination to the X.25 cloud. In this typical configuration, Cisco A tries to establish an SVC to Cisco B using its X.121 source address and a destination X.121 address of 311082191234 when it sends packets to 15.60.8.2.

Upon receipt of the setup request, Cisco B identifies the remote IP address from the source X.121 address and accepts the connection. Once the SVC is connected, each router uses it as a point-to-point data link for the identified destination.

The two X.25 attachments need complementary map configurations to establish the VC that will encapsulate IP datagrams.

X.25 Additional Configuration Tasks



Configure interface for X.25 Layer 3 parameters

- **Virtual circuits**
- **Packet size**
- **Window size**
- **Window modulus**

19

It may be necessary to perform additional configuration steps so that the router will work correctly with the service provider network. Crucial X.25 parameters are:

- Virtual circuit range—Incoming, two-way, and outgoing
- Default packet sizes—Input and output
- Default window sizes
- Window modulus

Configuring X.25 VC Ranges

	Range	Default	Command
PVCs	1-4095		x25 pvc *circuit*
SVC Incoming only	1-4095	0	x25 lic *circuit*
DCE initiated	1-4095	0	x25 hic *circuit*
SVC Two-way	1-4095	1	x25 ltc *circuit*
	1-4095	1024	x25 htc *circuit*
SVC Outgoing only	1-4095	0	x25 loc *circuit*
DTE initiated	1-4095	0	x25 hoc *circuit*

20

This table summarizes additional configuration tasks for virtual circuit number assignment. The complete range of virtual circuits can be allocated to PVCs or SVCs depending on your requirements. SVCs are commonly used.

If both limits of a range are zero, the range is unused.

The circuit numbers must be assigned so that an incoming range comes before a two-way range, both of which come before an outgoing range. Any PVCs must take a circuit number that comes before any SVC range. The following numbering scheme lists the proper order for these virtual circuit number assignment commands:

$1 \leq \text{PVCs} < (\text{lic} \leq \text{hic}) < (\text{ltc} \leq \text{htc}) < (\text{loc} \leq \text{hoc}) \leq 4095$

(Where lic is low incoming circuit number, hic is high incoming circuit number, ltc is low two-way circuit number, htc is high two-way circuit number, loc is low outgoing circuit number, and hoc is high outgoing circuit number.)

X.25 ignores any events on a VC number not in an assigned VC range; it considers the out-of-range VC as a protocol error. The network administrator specifies the VC ranges for an X.25 attachment. For correct operation, the X.25 DTE and DCE must have identically configured ranges. Numbers configured for any PVCs must also agree on both sides of an attachment (not necessarily end to end).

Configuring X.25 Packet Sizes

Router (config-if) #

x25 ips *bytes*

- **Specifies default incoming packet size**

Router (config-if) #

x25 ops *bytes*

- **Specifies default outgoing packet size**

21

The **x25 ips/ops** command sets the default maximum input/output packet size. The input and output values should match unless the network supports asymmetric transmissions.

x25 ips/ops Command	Description
bytes	Maximum packet size assumed for VCs that do not negotiate a size. Supported values are: 16, 32, 64, 128, 256, 512, 1024, 2048, and 4096. Default is 128 bytes.

If the stations of an X.25 attachment conflict on the VC's maximum packet size, the VC is unlikely to work.

Configuring Window Parameters

Router (config-if) #

x25 win *packets*

Router (config-if) #

x25 wout *packets*

- **Specifies default unacknowledged packet limits**

Router (config-if) #

x25 modulo *modulus*

- **Defines packet-level window counter limit**

22

Use the **x25 win/wout** command to set the default window size. The window size specifies the number of packets that can be received/sent without sending/receiving an acknowledgment. Both ends of an X.25 link must use the same default window size.

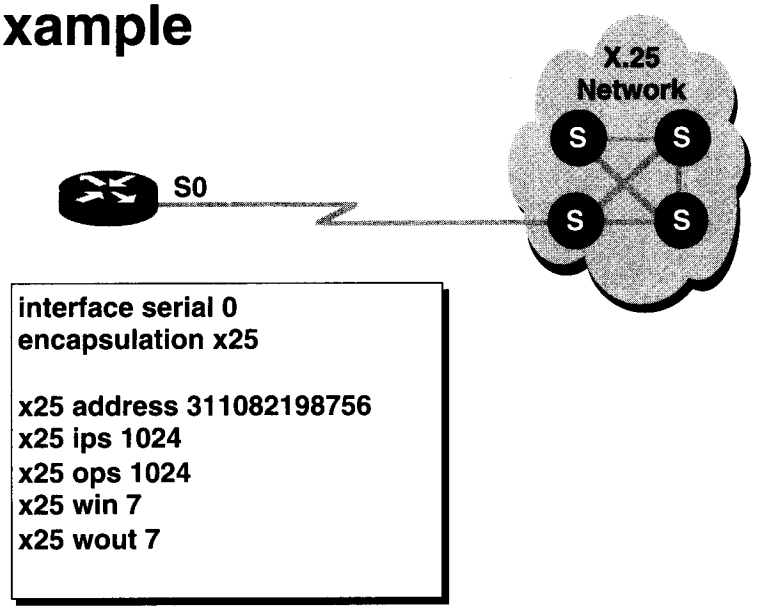
The **x25 modulo** command specifies the packet numbering modulus. It affects the maximum number of window sizes. The **x25 modulo** command specifies the data packet numbering modulo. Modulo 8 is widely used and allows virtual circuit window sizes up to 7 packets. Modulo 128 is rare, but allows VC window sizes up to 127 packets.

Both ends of an X.25 link must use the same modulo.

x25 win/wout Command	**Description**
packets	Packet window size, assumed for VCs that do not negotiate a size. Range is one to one less than the modulus. The default is two packets.

x25 modulo Command	**Description**
modulus	Either 8 or 128.

X.25 Additional Configuration Example



23

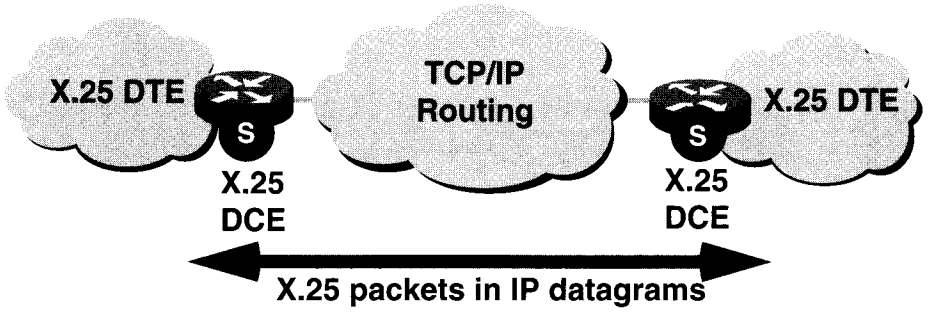
An X.121 address is assigned to interface serial 0. The input and output packet and window sizes and the maximum number of virtual circuits for any protocol are also defined.

In the example:

Command	Description
x25 address 311082198756	Specifies the address of the interface.
x25 ips/ops 1024	Sets both input and output default packet size to 1024 to match the values defined for the network attachment. Maximum value is 4096.
x25 win/wout 7	Sets both input and output window sizes to 7 to match the values defined for the network attachment.

The typical default packet size provided worldwide by PDNs is 128 bytes. In the United States and Europe, default packet sizes of 1024 are common. Other countries can also provide higher packet sizes. The Layer 3 default maximum packet size is subject to the limit that lower layers are able to support.

Setting Up the Router as a Switch



- **Router acts as local or remote switch**
- **Router switches X.25 traffic over TCP (XOT)**

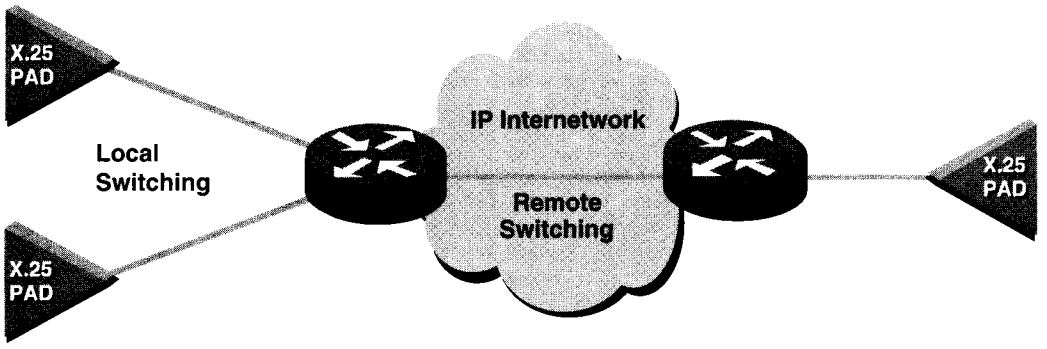
24

The router can be configured to switch X.25 traffic over a TCP connection.

In this mode, the backbone comprises routers switching IP datagrams. A few X.25 devices, such as PADs, connect to each other across the routed IP backbone network.

The switching performance of IP is higher than native X.25 switching equipment. This use of a TCP/IP cloud provides customers with high-performance, concurrent switching of X.25, IP, and other protocols.

X.25 Local and XOT Switching



Router (config) #

x25 route [***# position***] ***x.121-address*** [**cud** ***pattern***]
interface ***type-number***

25

X.25 traffic can be routed locally between serial ports. In this case, static routing statements map X.121 addresses to serial ports. The router allows X.25 interfaces attached to different ports to make SVC connections. This is called local X.25 switching.

Remote X.25 switching allows X.25 interfaces attached to different routers to establish SVCs and PVCs. This is accomplished by tunneling all the X.25 call setup and data traffic between routers in a TCP connection.

x25 route Command	Description
# position	(Optional) A positional value that specifies the line number in the table where the entry will be placed.
x.121-address	Destination X.121 address pattern.
cud *pattern*	(Optional) Call User Data (CUD) pattern, which is a printable ASCII string. Caution: This must be the value provided by the X.25 service provider.
type-number	The destination interface number, such as serial 0.

Monitoring X.25

```
Router# show interfaces serial 0
Serial0 is up, line protocol is up
  Hardware is MK5025
  Internet address is 183.8.128.129, subnet mask is 255.255.255.128
  MTU 1500 bytes, BW 56 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation X25, loopback not set
  LAPB DCE, state CONNECT, modulo 8, k 7, N1 12048, N2 20
       T1 3000, interface outage (partial T3) 0, T4 0
       VS 1, VR 1, Remote VR 1, Retransmissions 0
       IFRAMEs 1728559/1639143 RNRs 0/0 REJs 0/0 SABM/Es 3/2 FRMRs 0/0 DISCs 0/0
  X25 DCE, address 311012345678, state R1, modulo 8, timer 0
       Defaults: cisco encapsulation, idle 0, nvc 1
         input/output window sizes 2/2, packet sizes 128/128
       Timers: T10 60, T11 180, T12 60, T13 60, TH 0
       Channels: Incoming-only none, Two-way 1-1024, Outgoing-only none
       RESTARTs 3/3 CALLs 244+235/266+262/0+0 DIAGs 0/0
  Last input 0:00:00, output 0:00:00, output hang never
  Last clearing of "show interface" counters never
  Output queue 0/40, 0 drops; input queue 2/75, 0 drops
  Five minute input rate 0 bits/sec, 3 packets/sec
  Five minute output rate 0 bits/sec, 3 packets/sec
     3370943 packets input, 113376062 bytes, 0 no buffer
     Received 1971 broadcasts, 0 runts, 0 giants
     57 input errors, 57 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 --More--
```

26

Use the **show interfaces** command to display status and counter information about an interface. This serial interface has its encapsulation type configured for X.25 operation.

The output from this command also displays LAPB information.

Summary

X.25 defines the lower three layers of the OSI model

LAPB is the data-link protocol

Tunneling of other protocols inside X.25 is supported

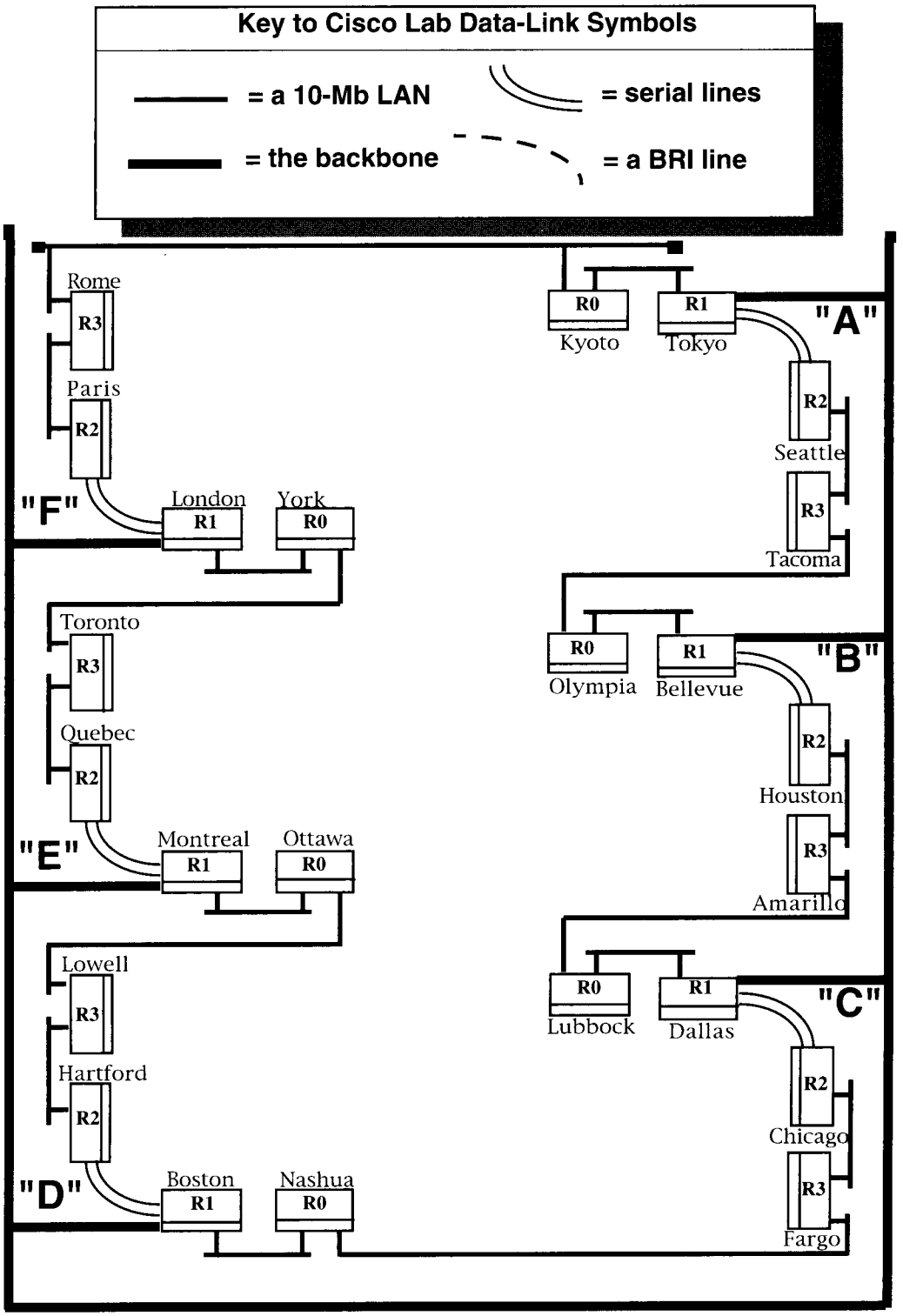
To configure an X.25 interface you must:

- Define the interface encapsulation
- Set critical parameter values for attaching to the PDN
- Configure the interface X.121 address
- Define any protocol to X.25 mapping

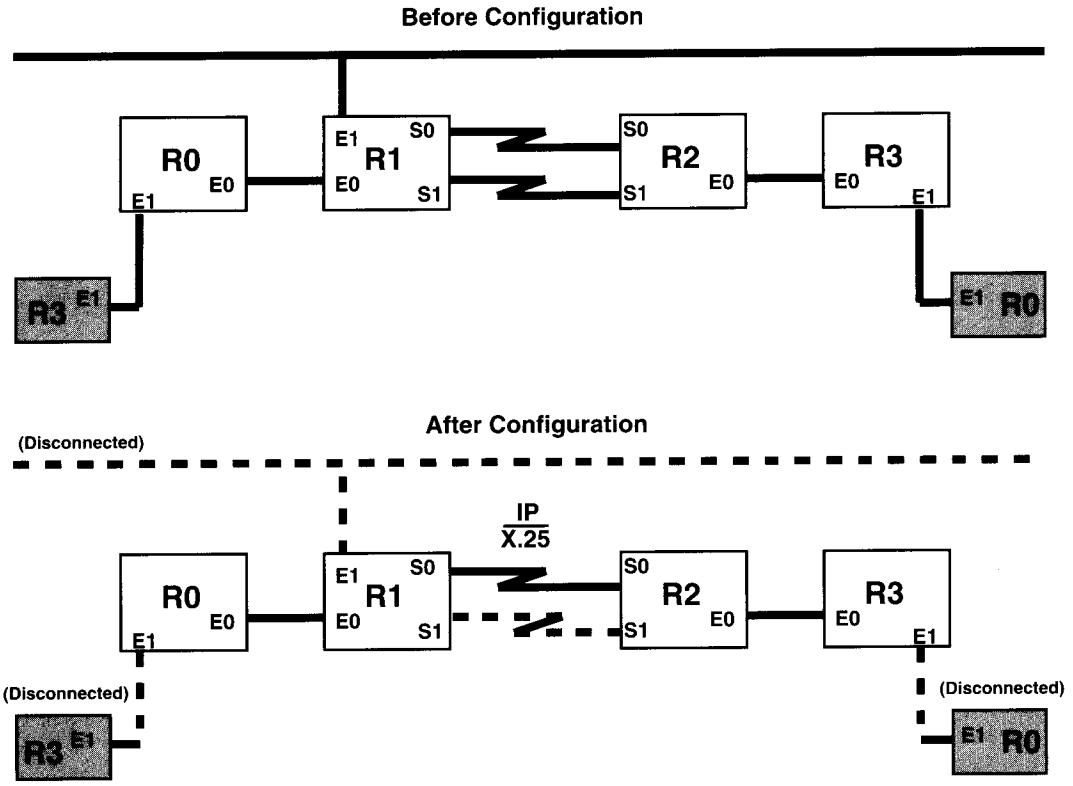
27

Lab: X.25 Implementation

Map of the Internetwork



X.25 Encapsulation Data Sheet



Objective: Configure X.25 on router interfaces.

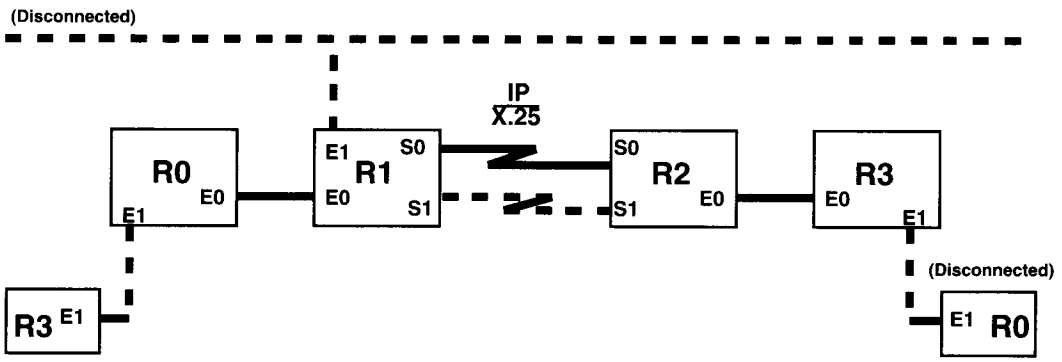
Objective: Monitor X.25 operation in the router.

Instructions: Configure X.25 encapsulation of IP between the S0 interface on R1 and the S0 interface on R2. To confirm that X.25 is working, turn off the E1 interfaces on all routers and the S1 interfaces between R1 and R2. If the configuration is correct, IP packets will still be able to travel between R0 and R3.

Use the assigned X.121 addresses for your own workgroup. Add four more digits to the prefix (for example, one S0 interface address on group A could be 311010101234.)

Group	X.121 Prefix
A	31101010....
B	31101011....
C	31101100....
D	31101101....
E	31101110....
F	31101111....

X.25 Encapsulation Implementation



X.121 Address R1 S0 _____

X.121 Address R2 S0 _____

Step 1 Use the **shut** command to close the S1-to-S1 link. Also shut all the E1 interfaces. Make sure that only S0 interfaces connect the R1 and R2 routers.

Step 2 On R1 interface S0, configure for **encapsulation x25.**

On R2 interface S0, configure for **encapsulation x25 dce**. Because this router will act as DCE, enter the command for a **clock rate 56000** (56 kbps).

Step 3 Set up X.121 addresses for your group using the information on the previous page. Enter the address on the graphic. Then configure the address on S0 using **x25 address**.

Step 4 Use **telnet** or **ping** to verify that communication between R0 and R3 has been interrupted.

Step 5 Configure the X.25 to IP mapping that indicates the target S0 address on the other side of the link. Use the command **x25 map ip** ***address x121-address*** **broadcast**.

Step 6 Monitor X.25 operation with the command **show interface s0**. Verify that the interface and the line protocol are both up.

Step 7 Use **telnet** or **ping** the router to verify that communication between R0 and R3 has been restored over the link with X.25 encapsulation.

Step 8 When done, return the encapsulation on S0 to the default HDLC and remove all commands related to X.25 from the running-configuration.

Remove the shuts on S1 interfaces. Also remove the shut on the E1 interface that connects the R1 router to the backbone.

CHAPTER 19

Configuring Frame Relay

Objectives

Upon completion of this module, you will be able to perform the following tasks:

Describe Cisco's implementation of Frame Relay

Recognize key Frame Relay terms and features

List the command to configure Frame Relay LMIs, maps, and subinterfaces

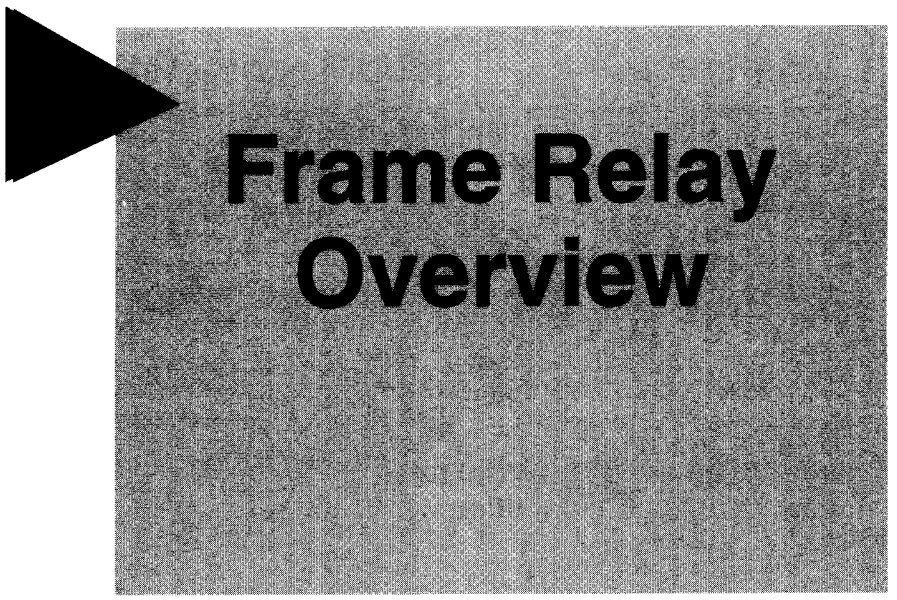
List the command to monitor Frame Relay operation in the router

2

This chapter discusses how to configure Frame Relay routing.

Sections:

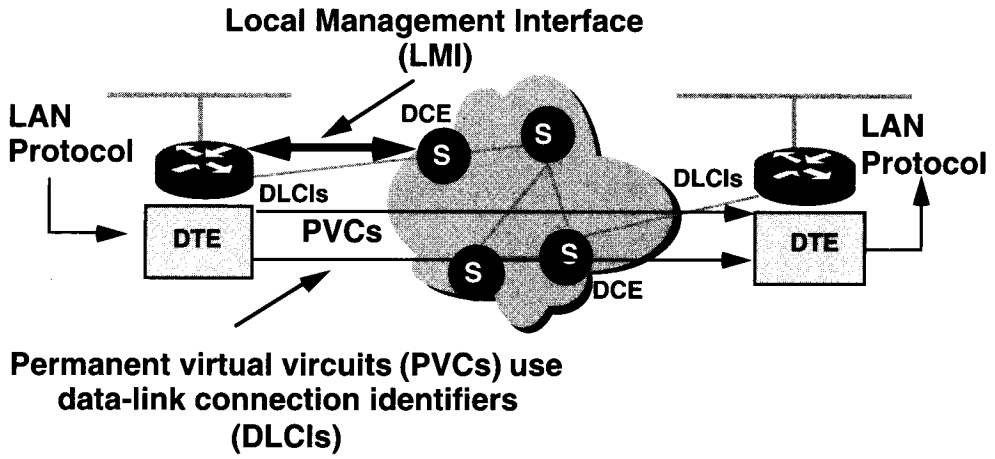
- Frame Relay Overview
- Configuring Frame Relay
- Answers to Exercises



3

Frame Relay Overview

Introduction to Frame Relay



4

Frame Relay operates like a streamlined, speeded-up descendant of X.25. In many industrialized countries, Frame Relay has been replacing the more complex, slower packet-switching services.

Regional Bell Operating Companies (RBOCs), alternate WAN carriers, and Post, Telephone, and Telegraph (PTT) providers have widely deployed a digital communication infrastructure that operates inside the WAN cloud.

At the same time, end-user devices at the edge of the WAN cloud increasingly demand wide-area connections that provide higher transmission speeds, lower network delays, and efficient bandwidth to accommodate bursty data.

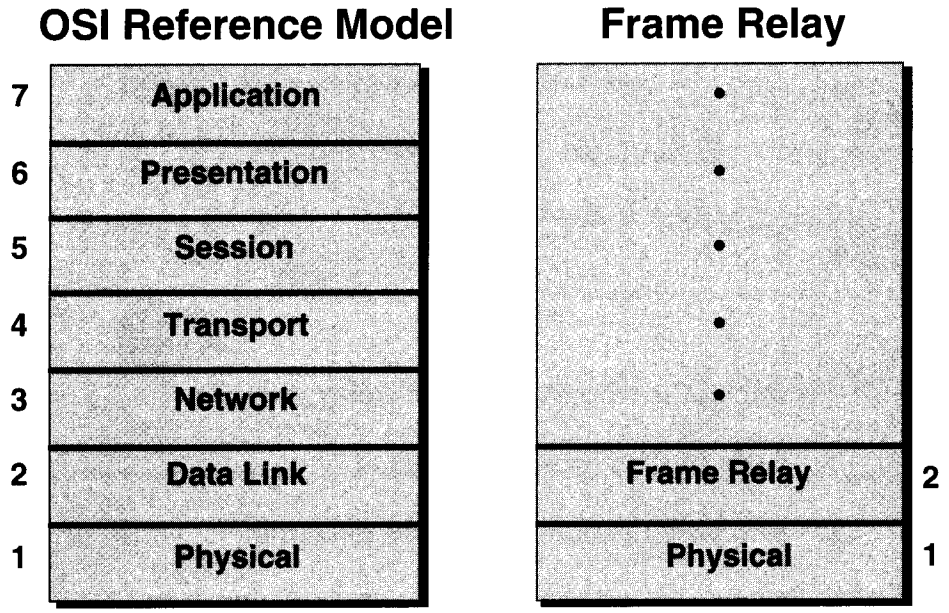
Frame Relay is based on virtual circuits (VCs). Because of its relatively high-speed throughput and minimal overhead, Frame Relay is well suited for connecting LANs across a WAN. Because the router encapsulates upper-layer data in Frame Relay, it provides a DTE connection to the communications cloud DCE, which is a Frame Relay switch.

Frame Relay operates over permanent virtual circuits (PVCs). This means that connections are static, provisioned by a configuration statement. Multiple PVCs can interconnect DTEs across the Frame Relay network to a destination.

A data-link connection identifier (DLCI) identifies each PVC. The DLCI provides the major addressing mechanism of the router's Frame Relay support to the Frame Relay WAN service.

Local Management Interface (LMI) refers to the overhead processing that sets up and maintains the connection between the router and the switch. It contains information about the PVC setup, status inquiries, and keepalive exchanges, as well as DLCI usage.

Frame Relay Stack



5

The core aspects of Frame Relay function at the lower two layers of the OSI reference model.

Using modern physical-layer facilities such as fiber media and digital transmission links, Frame Relay offers higher-speed WAN transmission for end stations, typically on LANs.

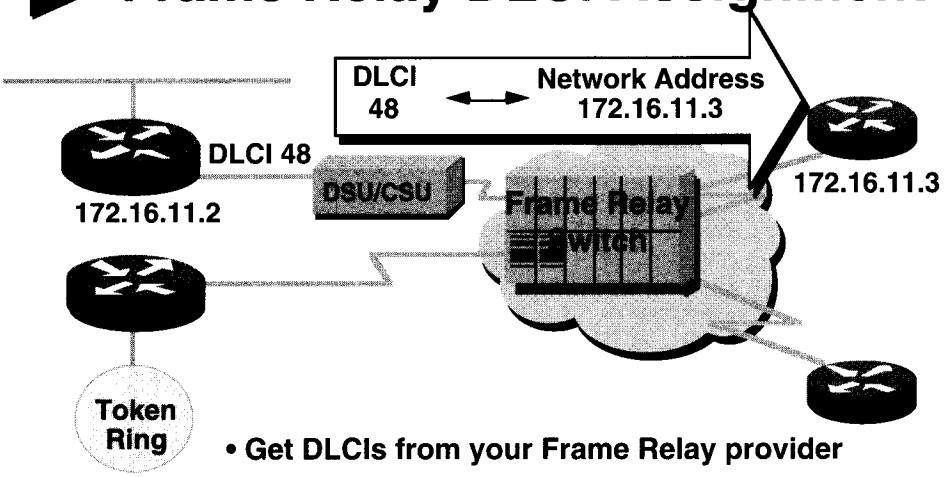
Working at the data link layer, Frame Relay encapsulates information from the upper layers of the OSI stack.

Frame Relay operations share some features with older WAN packet switching such as X.25. For example, a Frame Relay interface between the user and the network equipment will transmit and receive frames using first-in, first-out (FIFO) queuing on a statistically multiplexed circuit. Several logical connections, described as virtual circuits, can share the same physical link.

However, unlike X.25, Frame Relay offers a relatively high-speed, streamlined service:

- Transmission speeds for Frame Relay span a wide range of data rates. Typically, a Frame Relay link transmits data at 56 kbps or 64 kbps, with T1/E1 (up to 2 Mbps) becoming common; Digital Signal 3 (DS-3) speed (45 Mbps) is available from some service providers.
- Frame Relay streamlined service functions as a "best-effort" unreliable link, assuming that improved digital or fiber facilities allow forgoing time-consuming error-correction algorithms, acknowledgment schemes, and flow control corrections.

Frame Relay DLCI Assignment



- **Get DLCIs from your Frame Relay provider**
- **Each DLCI is locally significant**
- **Map your network addresses to DLCIs**
- **Map entry indicates static route to destination**

6

This graphic shows a closer look at a Frame Relay DLCI in operation. Two routers are separated by a Frame Relay cloud. The channel service unit/digital service unit (CSU/DSU) is a common intermediary device used for digital circuit connection and line interface. The large Frame Relay switch in the cloud represents a Frame Relay service provider.

Frame Relay as a public service is typically deployed by telephone companies such as RBOCs in the data communication market. Frame Relay can also be a network of privately owned switches. In either case, the Frame Relay provider sets up the DLCI numbers to be used by the routers for establishing PVCs.

DLCIs usually have local-only significance, meaning that any locally available number can be used at each location.

Also, certain DLCIs represent special functions: DLCI 1023 is specific for LMI use; and DLCIs 1019 to 1022 address multicast (one to several) as defined by the industry-common specification.

A network administrator configures an available DLCI number to map this provided Frame Relay number to a network address. For example, an administrator might map to an IP address of the interface on the right side router in the graphic. This mapping in the router points to a static route, which is the PVC to that remote router. For example, the administrator can configure a Frame Relay map for 172.16.11.3 using the PVC identified as DLCI 48.

Cisco LMI Support

ANSI	T1.617 Annex D
ITU-T (CCITT)	Q.933 Annex A (signaling)
Cisco	"Gang of four"

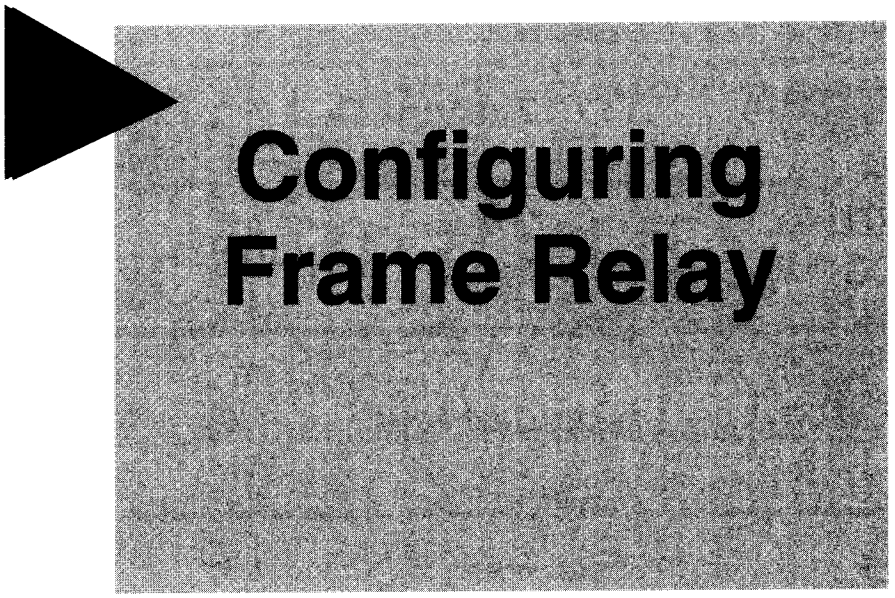
7

Cisco offers broad support to these major Frame Relay protocol variations:

- The American National Standards Institute's (ANSI's) accredited T1S1 committee in the United States describes Frame Relay signaling with T1.617 Annex D.
- The International Telecommunication Union Telecommunication Standardization Sector (ITU-T), formerly CCITT, uses the transmission standards sector to set Frame Relay signaling with Q.933 Annex A. This group began Frame Relay development in the mid-1980s as part of its ISDN research. Refer to this LMI as q933a in the router.
- Cisco refers to a consortium of the companies, nicknamed the "gang of four." These companies were Cisco, Digital Equipment Corporation, Northern Telecom, and StrataCom. Beginning in 1990, these companies worked together on Frame Relay technology to accelerate product introduction and interoperability.

  Extensions promoted by this gang of four include virtual circuit status messages (commonly adopted) and three other optional LMI extensions (multicasting, global addressing, and simple flow control).

An administrator setting up a connection to a Frame Relay network must choose the appropriate LMI from these three alternatives to ensure proper Frame Relay operation.



8

Configuring Frame Relay

Frame Relay Configuration

Router (config-if) #

encapsulation frame-relay [ietf]

- **Sets Frame Relay encapsulation**

Router (config-if) #

frame-relay lmi-type { ansi | cisco | q933a }

- **Selects LMI type**

9

Use the **encapsulation frame-relay** command to specify the data-link encapsulation type to be used on the serial interface communicating with the Frame Relay network.

Two different data-link encapsulations are supported:

- The default is the Cisco encapsulation developed by the gang of four. This default operates only with other Cisco routers.
- The Internet Engineering Task Force (IETF) encapsulation is specified in RFC 1294/1490. This encapsulation allows interoperation with other vendors' routers.

The encapsulation can be specified globally, as illustrated here, or on a circuit-by-circuit basis, as shown in the next graphic.

The standard Frame Relay encapsulation, as defined by the IETF, is derived from Point-to-Point Protocol (PPP). The default encapsulation on the Cisco router is proprietary.

Use the **frame-relay lmi-type** command to select the LMI type.

The router must be configured with the appropriate signaling to match the Frame Relay carrier implementation. All standard LMI signaling formats are supported:

- ANSI—Annex D defined by ANSI standard T1.617
- ITU-T (or q933a)—Annex A defined by Q.933
- Cisco—LMI defined by the gang of four (default)

Frame Relay Address Mapping

Router (config-if) #

frame-relay map *protocol protocol-address DLCI*
[broadcast] [ietf | cisco]

- **Defines how to reach a destination**

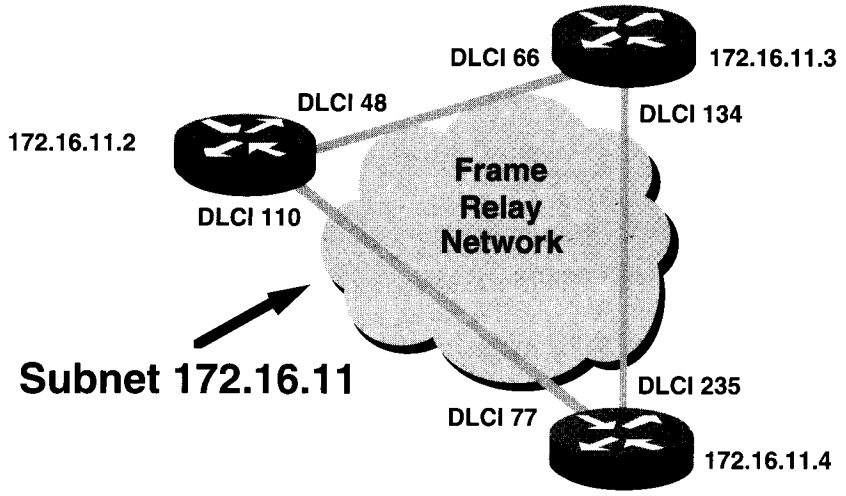
10

Use the **frame-relay map** command to statically map destination network protocol addresses to a designated DLCI.

frame-relay map Command	Description
protocol	Supported protocols: appletalk, clns, decnet, ip, xns, ipx, vines.
protocol-address	Address for the protocol.
DLCI	DLCI number of the virtual circuit.
broadcast	(Optional) Broadcasts should be forwarded when multicast is not enabled.
ietf	(Optional) Enables the IETF LMI.
cisco	(Optional) Enables the Cisco LMI (default).

This command is used in configurations where the Inverse ARP protocol is not used to dynamically determine the network protocol address at the other end of a virtual circuit.

Nonbroadcast Multiaccess (NBMA)



- **All routers appear as peers on a single subnet**
- **Assumes configuration with fully meshed virtual circuits**

11

One model for implementing Frame Relay in an internetwork is called nonbroadcast multiaccess (NBMA). The NBMA model makes all routers connected by virtual circuits peers on the same IP network or subnetwork. Because Frame Relay does not support broadcasting, the routers must copy all broadcasts and transmit on each virtual circuit.

For routing protocols that allow split horizon to be turned off, full connectivity can be achieved in a partial mesh configuration. For protocols such as AppleTalk RTMP, which do not allow split horizon to be turned off, connectivity is restricted between routers that are directly connected by virtual circuits.

Frame Relay Maps Example

Cisco A

```
interface serial 0
ip address  172.16.11.2   255.255.255.0
!
! enable frame relay, use the ANSI LMI
encapsulation frame-relay
frame-relay lmi-type ansi
! Note: for alternate ietf encap,  also use lmi-type ansi
!
!set up a static frame relay map - full mesh
!
frame-relay map  ip  172.16.11.3  48  broadcast
frame-relay map  ip  172.16.11.4  110  broadcast
```

12

In the example:

encapsulation frame-relay—Sets encapsulation type to Cisco (default).

frame-relay lmi-type ansi—Selects LMI to ANSI.

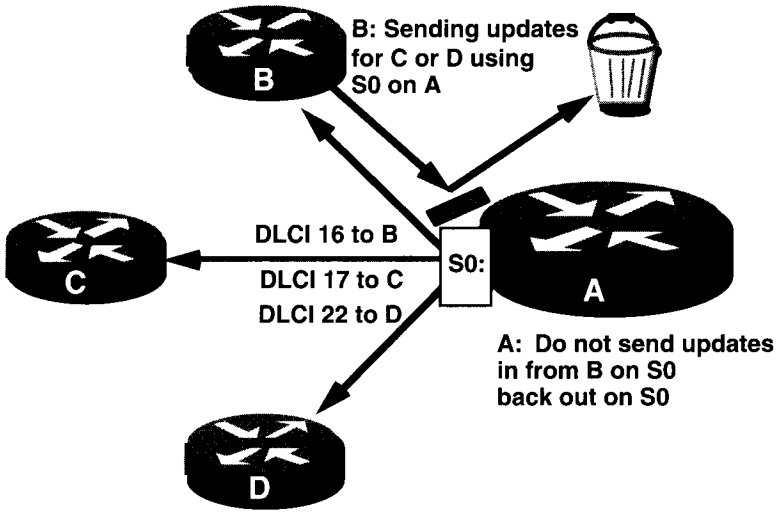
frame-relay map Command	Description
ip	Higher-level protocol.
172.16.11.3	Address being mapped.
48	DLCI used to reach the destination.
broadcast	Allows broadcasts, such as routing updates, to be forwarded.

IP traffic destined for 172.16.11.3 will use DLCI 48 to negotiate the Frame Relay cloud. Interface serial 0 will send broadcast traffic as well as IP traffic.

Cisco A is configured with a **frame-relay map** statement for every peer router. In this example, we show a fully meshed configuration with three routers.

Because of the overhead associated with copying broadcasts to a large number of peer routers, it is important to limit the number of routers in an NBMA group.

Split Horizon and Frame Relay



- **If you map DLCIs from A's SO, only updates to or from A can route on that interface (that is, not B to C or D)**

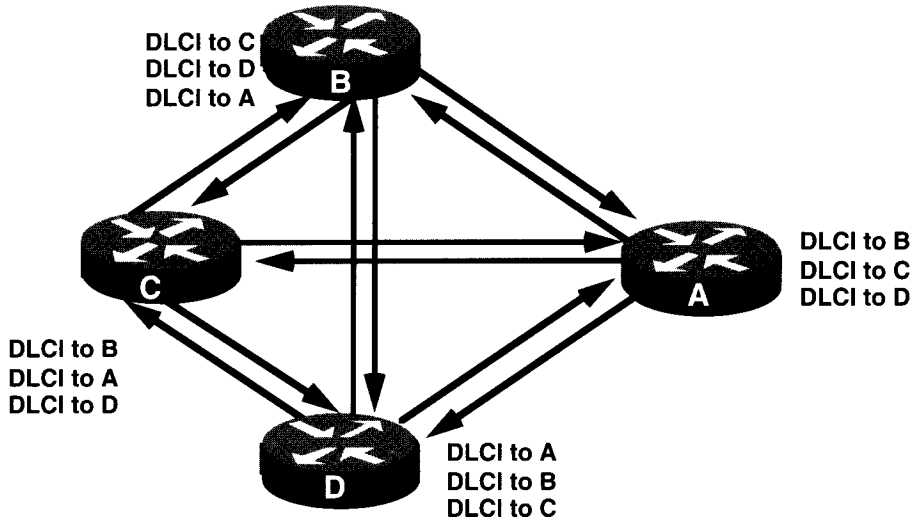
13

In an NBMA environment, routers trying to forward updates face another condition that can cause trouble. This condition comes from the operation of split horizon on a serial interface attached to WAN services.

With split horizon, if a router learns a route from an interface, it does not propagate information about that route back out that same interface. For Frame Relay, this condition applies for all routing protocols except those in the IP suite (for example, RIP, IGRP, Enhanced IGRP). Split horizon also applies to all service advertisements (for example, IPX SAP or GNS traffic, and AppleTalk ZIP updates).

If you map DLCIs from a serial interface, for example, S0 on router A, only updates from router A or to router A can traverse the S0 interface. If router B attempts to send updates for routers C or D through router A, then router A's split horizon process takes effect. Because the update comes in on S0, router A with split horizon will not allow it to go back out on S0.

Full Mesh for Frame Relay



- **Full connectivity using a full point-to-point mesh uses many PVCs and configuration statements**

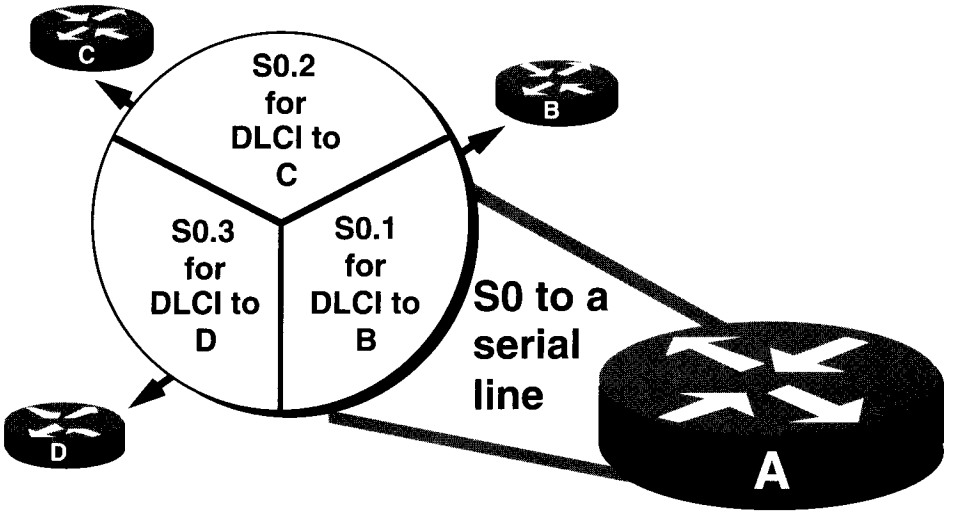
14

Because the split-horizon mechanism will not allow routers to send updates into and then out of the same interface, you could provision for connectivity by operating Frame Relay with a full mesh. This sets up a Frame Relay data link from every router to every other destination. Then at each router you configure a DLCI to each destination of that router.

However, this approach to connect routers over the Frame Relay WAN involves key disadvantages:

- The administrator must order many Frame Relay PVCs from the service provider. The service provider will need to install each provisioned PVC, and the enterprise will receive a bill for all charges. Then the enterprise faces ongoing, incremental bills for each PVC.
- The configuration at each router must contain mapping statements for each DLCI it uses. To represent all its Frame Relay destinations, the configuration of all routers using this full-mesh approach will require many map statements. This configuration might be difficult to set up and support.

An Alternative: Subinterfaces



- **Routers need to bypass split horizon on S0**
- **Define logical subinterfaces on the serial line**

15

An NBMA WAN environment needs to act like a LAN regarding its multiaccess operations. However, split horizon does not allow multiaccess updates into, and then out from, the same single serial line. Although routers need to get around split horizon for updates that use the WAN, the alternative of provisioning a full mesh may be impractical.

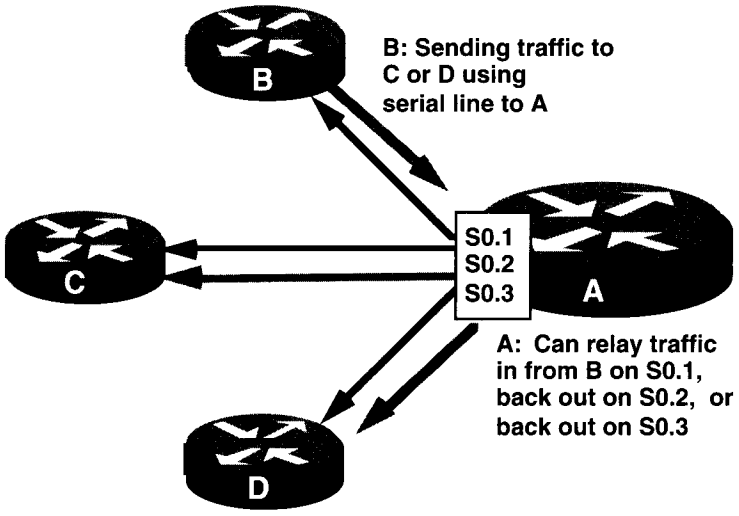
Another alternative establishes a number of virtual interfaces on a single physical serial interface. These virtual interfaces are logical constructs called subinterfaces.

You define these logical subinterfaces on the serial line. Each subinterface uses a DLCI that represents the destination for a Frame Relay PVC on your network. After you configure the Frame Relay interface DLCI on the subinterface, your router must associate one or more protocol addresses from the destination to the DLCI.

Keep in mind that you have still defined only the single S0 physical interface on router A. However, on that single S0, you have now defined an S0.1 subinterface for the Frame Relay DLCI to router B, an S0.2 subinterface for router C, and an S0.3 subinterface for router D.

v10.2 or Greater

Partial Mesh for Frame Relay



- **Map DLCIs with A's subinterfaces to connect all routers with fewer DLCIs and a simpler configuration**

16

When you define logical subinterfaces on a single physical interface, Frame Relay operates using a partial-mesh design.

To do so, you associate the DLCI for a destination to a subinterface. Use one DLCI and one subinterface for each destination router.

With subinterfaces configured, routers can connect with each other and send updates. Routers bypass the split horizon in effect for the single physical interface on router A's S0.

As a result you can connect all routers without needing a separate Frame Relay PVC between each router. The overall configuration to accomplish these connections is much simpler—you no longer need a map statement for each protocol address on each destination of each router.

Subinterface Configuration

Router (config) #

interface *type .subinterface-number* point-to-point

- **Defines the logical subinterface for Frame Relay and enters the interface configuration mode**

Router (config-if) #

frame-relay interface-dlci *dlci* broadcast

- **Assigns a DLCI to the Frame Relay subinterface on the router**

17

Before you can configure and use Frame Relay subinterfaces, you must first have a physical interface set up with encapsulation for Frame Relay. The commands and descriptions for Frame Relay subinterfaces follow. The first command defines the subinterface.

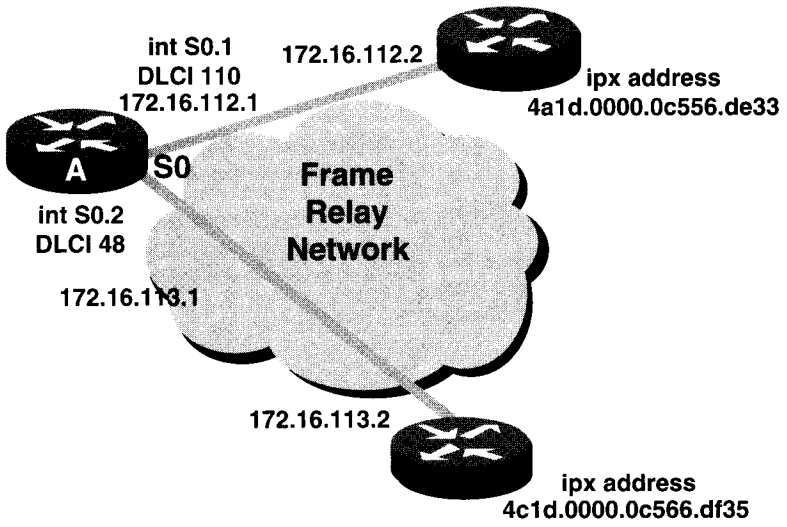
Command	Description
type	Any interface suitable for Frame Relay. Usually a serial interface.
.subinterface-number	*number* refers to the number of the physical interface; following the dot, *subinterface* is a unique integer on that interface.
point-to-point	This required keyword specifies that the subinterface refers to a single Frame Relay destination; the alternative argument is **multipoint.**

The **frame-relay interface-dlci** command assigns a Frame Relay DLCI to the subinterface.

Command	Description
dlci	The DLCI you designate to indicate the destination on the subinterface you defined with the first command.
broadcast	Allows the subinterface to forward broadcasts, such as routing updates.

Follow these commands by defining a destination's network address that Frame Relay will represent using the DLCI.

Frame Relay with Subinterfaces



- **Each Frame Relay subinterface uses its own subnet**

18

When you configure subinterfaces and Frame Relay DLCIs, the network architecture that results uses a different subnet for the link on each subinterface, as the graphic shows.

- On router A, the subinterface S0.1 uses DLCI 110 on IP subnet 172.16.112.0 (assuming 8 bits of subnet mask).
- For subinterface S0.2, DLCI 48 connects to 172.16.113.0.

This design differs from the approach you saw earlier with point-to-point mapping for NBMA. In that configuration, all routers acted as peers on a single subnetwork. The configuration used fully meshed PVCs.

However, when you use Frame Relay with subinterfaces, only the two routers on a PVC act as subnet peers. The Frame Relay configuration contains multiple subnetworks.

The DLCI on the subinterface represents one or more destination protocol addresses.

- On router A, DLCI 110 refers to the destination IPX network 4a1d.
- DLCI 48 refers to the destination IPX network 4c1d.

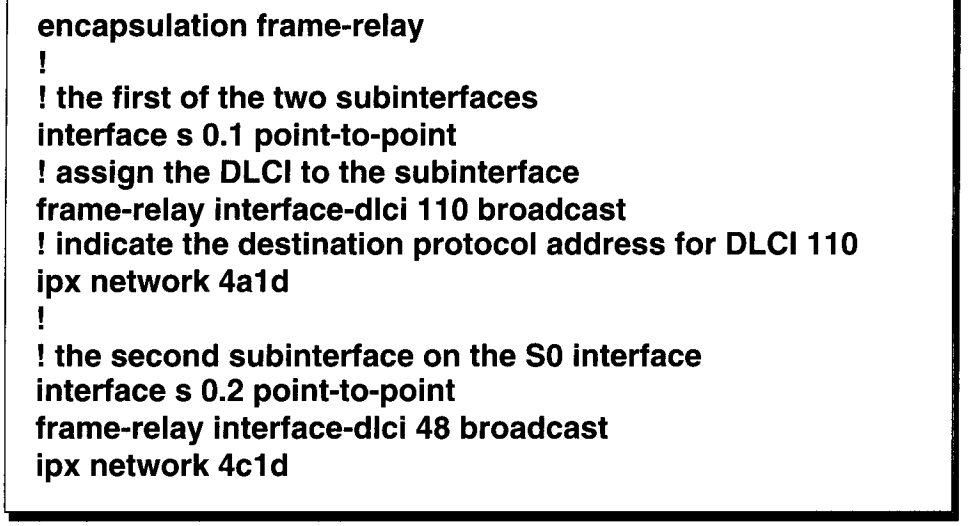
The next page shows the configuration commands used to implement this configuration.

A full mesh is no longer necessary for full update connectivity. No Frame Relay facility directly connects the two routers on the right. Using this approach saves the organization the initial and ongoing expenses otherwise necessary with a full-mesh network.

Subinterface Configuration Example

Cisco A

```
interface serial 0
encapsulation frame-relay
!
! the first of the two subinterfaces
interface s 0.1 point-to-point
! assign the DLCI to the subinterface
frame-relay interface-dlci 110 broadcast
! indicate the destination protocol address for DLCI 110
ipx network 4a1d
!
! the second subinterface on the S0 interface
interface s 0.2 point-to-point
frame-relay interface-dlci 48 broadcast
ipx network 4c1d
```



To configure Frame Relay subinterfaces, you start with the same commands you saw earlier. This example assumes that the Frame Relay LMI uses the default encapsulation *cisco*. In the example:

The **interface s 0.n point-to-point** command assigns a subinterface on the designated interface (S0).

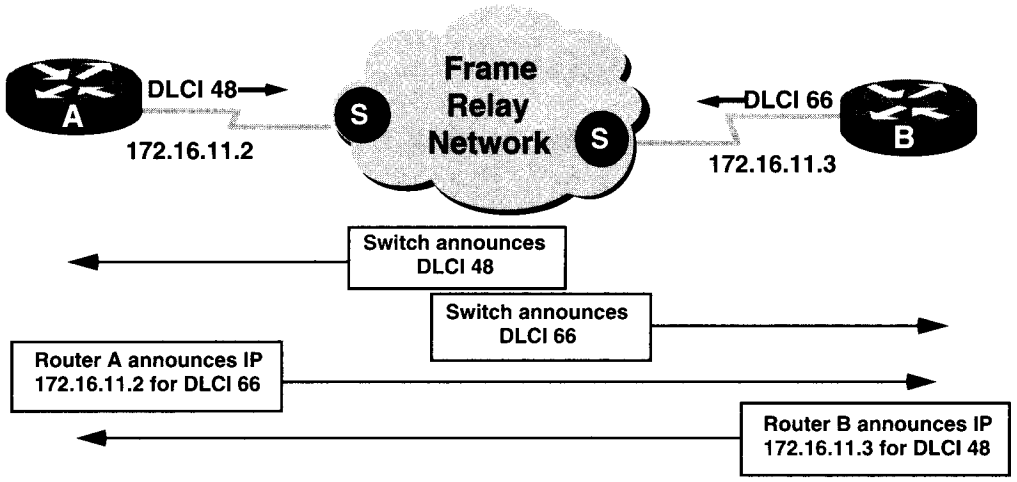
n	Subinterface number from 1 through 4294967293.
point-to-point	Establishes the type of the subinterface.

The **frame-relay interface-dlci nn broadcast** command sets the DLCI to use on the subinterface.

nn	Locally unique number from the DLCIs provided by the Frame Relay network service.
broadcast	Indicates that broadcast traffic can use the DLCI to the destination.

The **ipx network *nnnn*** command sets the network number. The subinterface DLCI refers to this destination.

Inverse ARP for Network Discovery



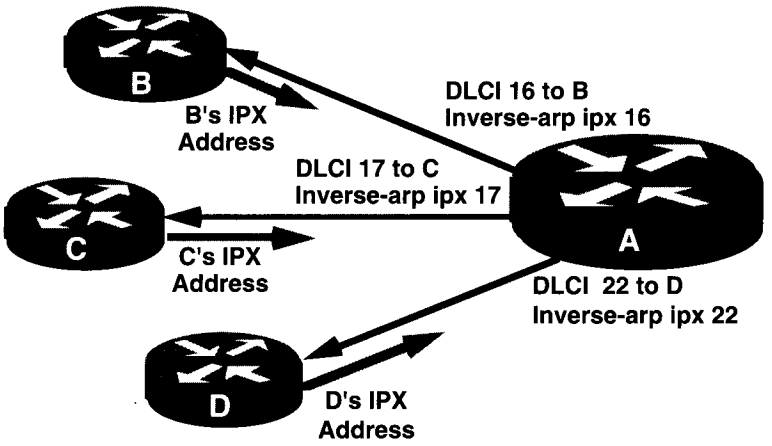
- **This auto-discovery of remote destination addresses simplifies Frame Relay configurations**

20

Configurations using either NBMA groups or subinterface DLCIs can be simplified through use of the Inverse ARP protocol. With Inverse ARP, the router needs to know only its own network protocol address on the NBMA network or subnet.

The router learns about the virtual circuits through LMI signaling from the Frame Relay switch. The router then learns the network address of each peer router by sending and receiving Inverse ARP messages on each added DLCI.

Using Inverse ARP for DLCIs



- **Frame Relay Inverse ARP is on by default once you specify DLCIs**
- **Inverse ARP resolves protocol addresses of remote routers for local DLCIs**

21

As soon as you specify DLCIs for Frame Relay, Inverse ARP automatically starts.

With Inverse ARP, the process resolves to a network address when given a DLCI. The router announces a network address and DLCI. The Frame Relay Inverse ARP allows the Frame Relay network to propagate the information.

Because Inverse ARP for Frame Relay is on by default, if you need to disable Inverse ARP on a local DLCI, use the **no frame-relay inverse-arp** command.

This configuration replaces the need for **frame-relay map** commands. However, any entries resulting from **frame-relay map** commands continue to establish static routes.

This configuration also replaces the need for entering specific network protocol address statements for subinterface configurations. However, any specific addresses you enter take precedence over any addresses for that protocol resolved by Inverse ARP.

The lines of text that describe the various arrows on the graphic are not commands the administrator must enter. Instead, they show the status of information that Inverse ARP uses for Frame Relay networks.

Showing a Frame Relay Interface

```
Router# show int s 0

Serial 0 is up, line protocol is up
  Hardware is MCI Serial
  Internet address is 172.16.11.2, subnet mask is 255.255.255.0
  MTU 1500 bytes, BW 56 Kbit, DLY 20000 usec, rely 252/255, load 1/255
  Encapsulation FRAME-RELAY, loopback not set, keepalive set (10 sec)
  LMI DLCI 1023, LMI sent 1, LMI stat recvd 0, LMI upd recvd 0
  Last input 0:04:42, output 0:00:07, output hang never
  Last clearing of "show interface" counters never
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 0 bits/sec, 0 packets/sec
  Five minute output rate 0 bits/sec, 0 packets/sec
    6019 packets input, 305319 bytes, 0 no buffer
    Received 2973 broadcasts, 0 runts, 0 giants
    7 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 7 abort
    8595 packets output, 3499314 bytes, 0 underruns
    0 output errors, 0 collisions, 10 interface resets, 0 restarts
    17 carrier transitions
```


Using the **show interface serial** command displays a snapshot of current Frame Relay settings. In particular, note the encapsulation set to Frame Relay, and the bandwidth set to 56 kbps. Also note that LMI transactions will use DLCI 1023.

Several other **show** and **debug** commands for monitoring Frame Relay operation from your router are described in the Cisco Connection Documentation, Enterprise Series CD-ROMs.

Monitoring Frame Relay

```
Router#terminal monitor
Router#no logging console
Router#debug frame-relay lmi

Serial 0 (out): StEnq, clock 20212760, myseq 206, mineseen 205, yourseen 136, DTE up
Serial 0 (in): Status, clock 20212766, myseq 206
RT IE 1, length 1, type 1
Serial 0 (out): StEnq, clock 20212770, myseq 207, mineseen 206, yourseen 138, DTE up
Serial 0 (in): Status, clock 20212776, myseq 207
RT IE 1, length 1, type 0
KA IE 3, length 2, yourseq 146, myseq 298
PVC IE 0x7, length 0x6, dlci 48, status 0, bw 56000
PVC IE 0x7, length 0x6, dlci 58, status 0, bw 56000
PVC IE 0x7, length 0x6, dlci 110, status 4, bw 56000
```


Your Frame Relay configuration enables the router to interface the Frame Relay service provider network. The router exchanges LMI packets with the provider's Frame Relay switch. Use the **debug frame-relay lmi** command to see an indication of the exchanged information between your router and your Frame Relay service provider.

The sample display from this **debug** command includes the following information:

Command	Description
Serial 0 (out)	Indicates an LMI packet sent out from the router on that interface.
DTE up	Frame Relay line protocol is up for the user-side interface.
Serial 0 (in)	Indicates an LMI sent by the provider switch into the router.
type 1 (or type 0)	Status update is abbreviated (type 1), or full (type 0).
PVC IE.....dlci 48, status 0	Full status update PVC information element on DLCI 48 shows that DLCI has been added to the network and is inactive.
bw 56000	PVC for the DLCI uses a 56-kbps Frame Relay facility.

Summary

Use a locally significant DLCI as an indicator of the ultimate destination of a Frame Relay PVC

Cisco supports different Frame Relay LMIs:

- **ANSI (Annex D)**
- **CCITT (Annex A)**
- **Cisco (LMI)**

Define static PVC routes with Frame Relay maps

Alternately, define subinterfaces for interface DLCIs to avoid split horizon on routing and SAP updates

Inverse ARP, on by default, auto-discovers remote protocol addresses for local DLCIs

Monitor Frame Relay with *show* and *debug* commands

24

Exercise: Frame Relay Review

Objective: Describe Cisco's implementation of Frame Relay.

Objective: Recognize key Frame Relay terms and features.

Problem 1

Entries in the table list the names of a Cisco Frame Relay implementation feature or term in column 1. Column 2 statements describe or define the function.

In the left column (labeled Write Letters), write the answer letter identifying the correct statement in column 2 that describes the given feature or term. For example, for item 2, write *I* in the blank space if you think item 2's description or function matches the statement in item *I*.

Note Column 2 intentionally contains extra statements.

Write Letter	Column 1 Feature or Term	Column 2 Description or Function
1._____	LMI	A) A locally significant identifier that indicates a Frame Relay link to a destination network address.
2. _____	Inverse ARP	B) An approach for implementing Frame Relay that makes all routers accessing Frame Relay part of the same IP subnet.
3. _____	DLCI	C) A designation of the subinterface that provides nonbroadcast access to multiple routers.
4. _____	IETF	D) The LMI developed by the "gang of four"—Cisco, Digital, Northern Telecom, and StrataCom.
5. _____	PVC	E) The overhead processing that sets up and maintains the connection between a Frame Relay DTE and DCE.
6. _____	NBMA	F) A local management interface type for Frame Relay proposed by the International Telecommunications Union Telecommunication Standardization Sector (ITU-T).
7. _____	S0.1	G) A nondefault Frame Relay encapsulation option that features framing interoperability between different vendors' routers.
8. _____	q933a	H) A static Frame Relay circuit that is explicitly provisioned by use of a configuration statement.
		I) Automatic discovery function that returns the remote-side network address when given a local DLCI.
		J) Integrates voice and data services on digital facilities using 4-bit symbols rather than octets in its framing.
		K) A subinterface for Frame Relay that overcomes the problems of full-mesh configurations and split-horizon blocking updates.

Problem 2

Objective: List the command to configure Frame Relay LMIs, maps, and subinterfaces.

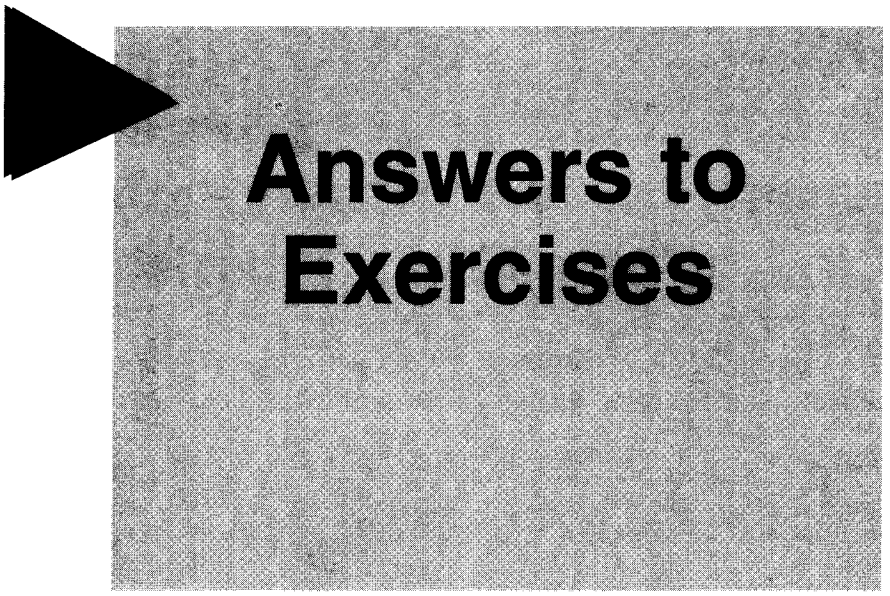
Objective: List the command to monitor Frame Relay operation in the router.

1. Write the command that would show you the DLCI used for LMI.

_____

2. Write the command to monitor LMI.

_____



27

Answers to Exercises

Exercise: Frame Relay Review

Problem 1

1. Local Management Interface—E
2. Inverse Address Resolution Protocol—I
3. Data-link connection identifier—A
4. Internet Engineering Task Force—G
5. Permanent virtual circuit—H
6. Nonbroadcast multiaccess—B
7. Serial interface 0.1—K
8. Q933 Annex A—F

Problem 2

1. show interface
2. setup

CHAPTER 20

AutoInstalling Configuration Data

Objectives

Upon completion of this chapter, you will be able to:

Describe how to use the AutoInstall procedure to remotely configure a new router

Identify where the new router acquires its IP address, host name, and configuration

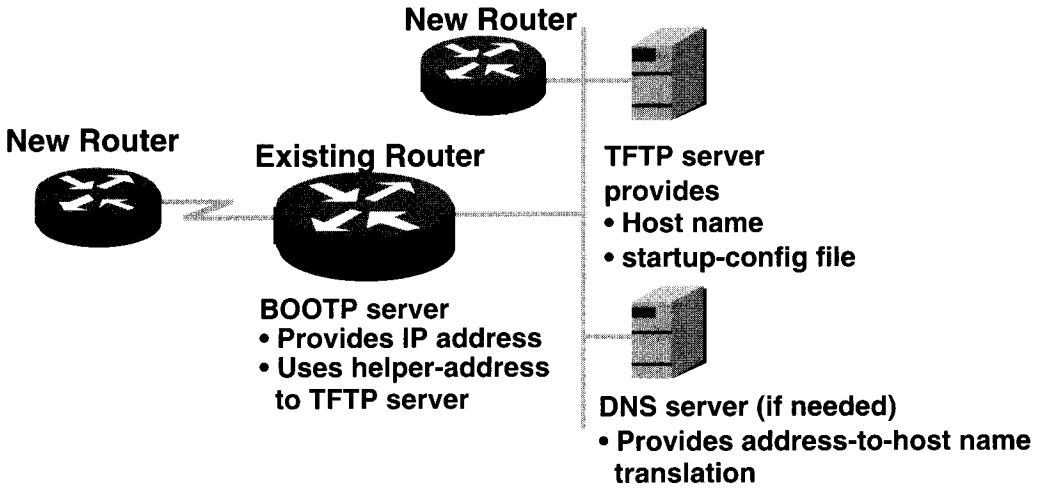
Download a configuration file over the following:

- **LAN link**
- **HDLC serial connection**

2

This chapter describes how to use the AutoInstall feature to configure a router. It explains where a router acquires its IP address, host name, and configuration.

New Router AutoInstall Overview



- **Configure a new router automatically and remotely**

3

The AutoInstall procedure allows a network administrator to configure a router automatically and remotely over the network. This configuration is most useful for establishing new routers in remote locations where branch office staff members have limited networking knowledge and skills.

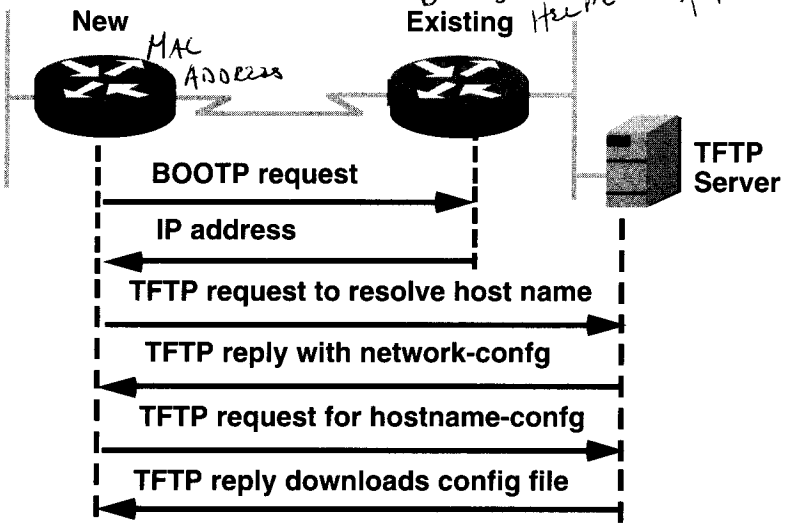
The new router must be connected to an existing router on either a WAN or LAN link. Both existing and new routers must be running Cisco IOS Release 9.1 or later for encapsulations other than Frame Relay. For Frame Relay encapsulation, both routers must be running Cisco IOS Release 10.3 or later.

The existing router acts as a Bootstrap Protocol (BOOTP) or Reverse Address Resolution Protocol (RARP) server. It must be set up to help the new router acquire its IP address. This existing router also contains a helper address for the TFTP server.

Note The new router configuration files must reside on the TFTP server. Prepare new router configuration files for AutoInstall in the Cisco IOS software configuration mode. Move your new router configuration files using the **copy running-config tftp** command to store the current configuration in RAM on a network TFTP server.

This server provides a host name for the address presented by the new router. If this IP address-to-host name translation does not occur on the TFTP server, then the new router uses a Domain Name System (DNS) server. The new router configuration is downloaded from a reachable TFTP server to the new router.

AutoInstall Procedures



- **The new router acquires its IP address, host name, and configuration**

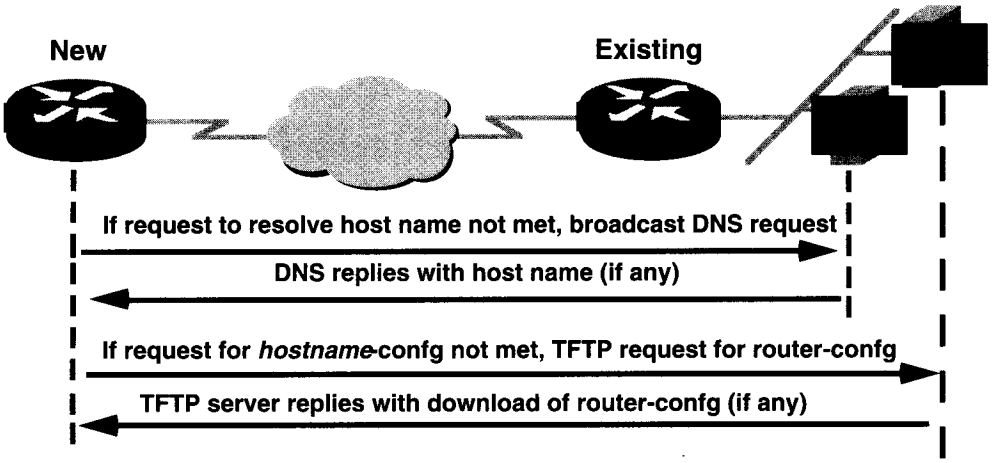
4

The AutoInstall procedure has several steps. First, the new router sends a BOOTP request for an IP address. The new router learns its IP address from the first valid BOOTP or RARP reply.

Once it has obtained an IP address, the new router requests a translation by the TFTP server to resolve this IP address into a host name. The response to this request comes in the form of a network-confg file containing the host name for the new router.

The new router uses its newly acquired host name to request the hostname-confg file that contains its specific configuration entries. The TFTP server downloads this file to the new router.

Fallback Requests for AutoInstall



- **If host name resolution from TFTP network-confg fails, the new router sends a request to the DNS server**
- **If the new router cannot get host name-specific confg, it sends a TFTP request for the more generic router-confg**

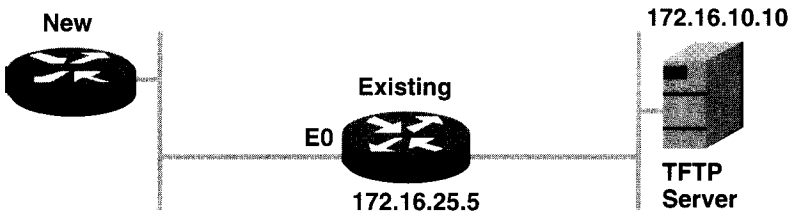
5

Prior discussions outlined AutoInstall operating in the most common scenarios. However, the AutoInstall process also includes several fallback requests to use if a common scenario fails to provide the proper response to the new router's requests.

If the host name request to the TFTP server fails to provide the new router with a host name, it will fall back to another request procedure. This sends a request to the DNS server to obtain IP address-to-host name translation.

Later, if the new router requests a hostname-confg file, but the TFTP server cannot send the requested file, it will send a more generic configuration in a router-confg file. Then the administrator can log in to the new router and make any specific configuration changes necessary for the new router.

LAN AutoInstall Example




```
interface ethernet 0
ip address  172.16.25.5  255.255.255.0
ip helper-address  172.16.10.10
```

Supported interfaces: Ethernet, Token Ring, FDDI

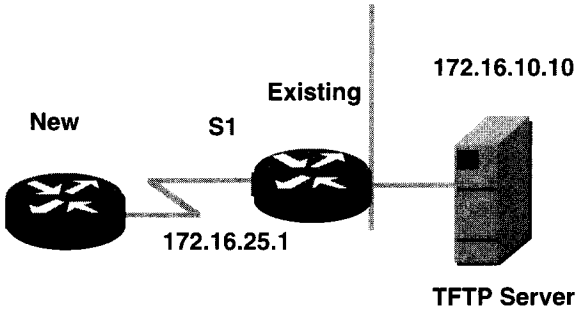
6

A new router can AutoInstall from an existing router and TFTP server using an Ethernet, Token Ring, or FDDI interface. The example commands shown are entries on the existing router.

Command	Description
interface ethernet 0	Defines an Ethernet interface on the existing router.
ip address 172.16.25.5 255.255.255.0	Defines the IP address for Ethernet interface 0 on the existing router.
ip helper-address 172.16.10.10	Defines the address of the TFTP server; all incoming TFTP requests at this interface are then forwarded to this address.

WAN AutoInstall Example

Using HDLC




```
interface serial 1
ip address  172.16.25.1 255.255.255.0
ip helper-address  172.16.10.10
```

- **Supported interfaces: HDLC, Frame Relay, HSSI with Frame Relay**

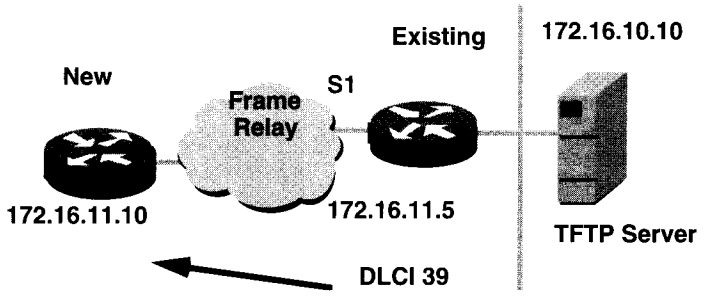
7

A new router can AutoInstall from an existing router and TFTP server across a WAN. The example command entries are shown for the existing router that uses HDLC.

Command	Description
interface serial 1	Defines serial interface 1 on the existing router.
ip address 172.16.25.1 255.255.255.0	Defines the IP address and its subnet mask for serial interface 1 on the existing router.
ip helper-address 172.16.10.10	Defines the address of the TFTP server; all incoming TFTP requests at this interface are then forwarded to this address.

WAN AutoInstall Example (cont.)

Using Frame Relay




```
interface serial 1
ip address  172.16.11.5 255.255.255.0
ip helper-address  172.16.10.10
encapsulation frame-relay
frame-relay map ip  172.16.11.10  39
```

8

In this example, the existing router and new router connect over a Frame Relay link. Command entries to set up AutoInstall for this environment are as follows:

Command	Description
interface serial 1	Defines serial interface 1 on the existing router.
ip address 172.16.11.5 255.255.255.0	Defines the IP address and its subnet mask for serial interface 1 on the existing router.
ip helper-address 172.16.10.10	Defines the address of the TFTP server; all incoming TFTP requests at this interface are then forwarded to this address.
encapsulation frame-relay	Defines Frame Relay encapsulation to be the Cisco-proprietary type instead of the type defined by the Internet Engineering Task Force (IETF).
frame-relay map ip 172.16.11.10 39	Statically maps the new router's IP address 131.108.11.10 to its designated data-link connection identifier (DLCI) 39.

Summary

Use AutoInstall to download to a remote router over:

- **LAN**
- **HDLC**
- **Frame Relay**

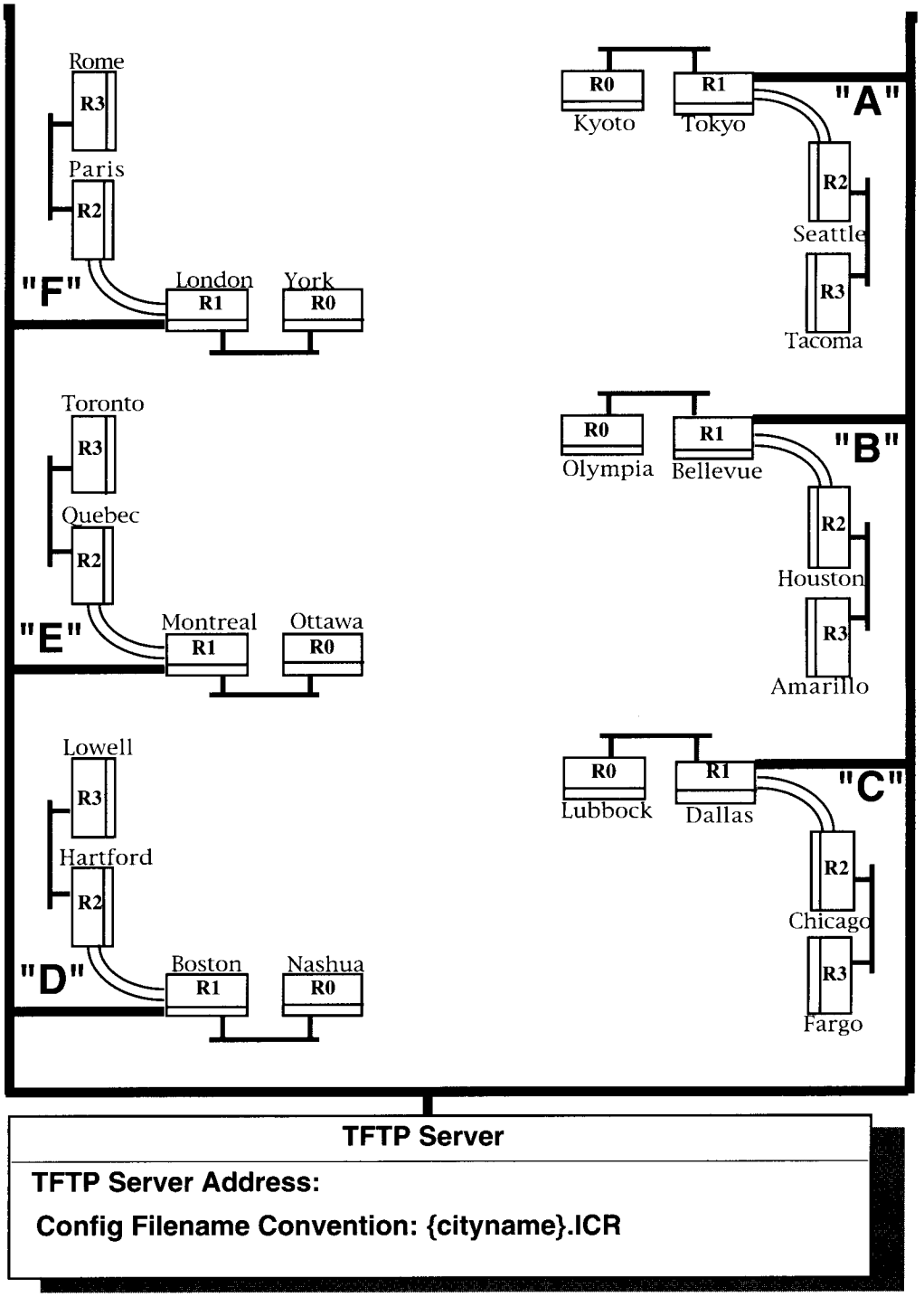
With AutoInstall, remote routers can get their:

- **IP address**
- **Host name**
- **Cisco IOS software configuration**

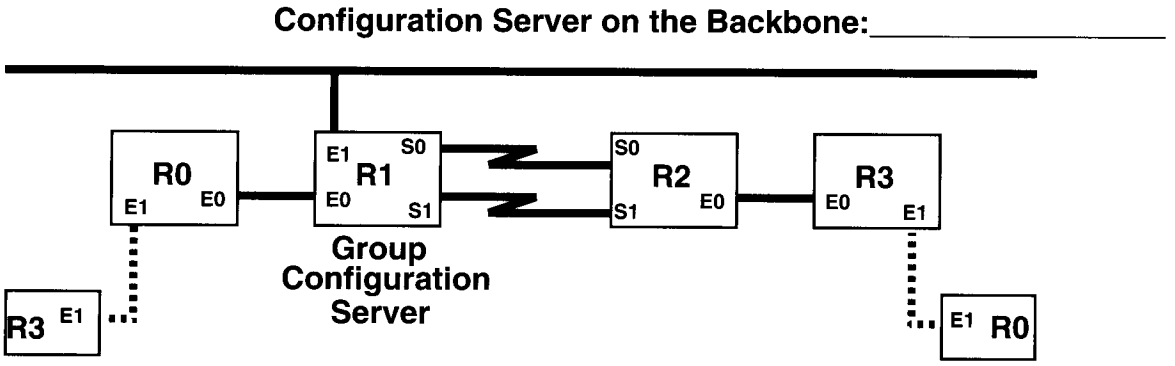
9

Lab: Configuring from a TFTP Server

AutoInstall Configurations from TFTP Server



AutoInstall Configuration Data Sheet



Objective: Download a configuration file over a LAN link or HDLC serial connection.

Instructions: This lab has two parts. Part 1 sets up the R1 router to be the group configuration server for group configuration files. Download the original class configurations for each group router to flash on the R1 router. Enable the R1 router to allow flash TFTP requests.

Part 2 uses the group configuration server. TFTP copy the original class configuration files to startup-config on each of the group routers. Then each router in the group can revert to the original configurations as the running-config on each router.

Part 1: Set up R1 as the group configuration server.

Step 1 On R1, interface E1, enter the command **no shut**. On the other routers, verify that no interfaces are open except those within the group.

Step 2 Determine the IP address of the classroom configuration TFTP server on the backbone. Write this IP address in the graphic. Use the **ping** command to make sure that you can reach this server.

Step 3 On each router starting with R0, identify the name of the original configuration file for the router on the classroom configuration server. Enter the filename in the table.

Router in Group	Configuration Filename
R0	
R1	
R2	
R3	

Step 4 On R1, use the command **show flash** to make sure you have at least 10,000 bytes of flash available to hold the group's router configuration files.

Step 5 On the R1 router, use the command **copy tftp flash** to begin downloading the configuration filename.

Step 6 Enter (or accept) the address of the remote host. This is the address of the configuration server on the backbone.

Enter the startup configuration name for the source file and accept it as the destination name. Confirm the name and address that will be used for downloading.

Step 7 When you see the question "Erase flash device before writing? [confirm]," press **Control-C**

Step 8 When you see the question "Copy 'filename' from server as 'filename' into Flash WITHOUT erase? [yes/no]," type **yes.**

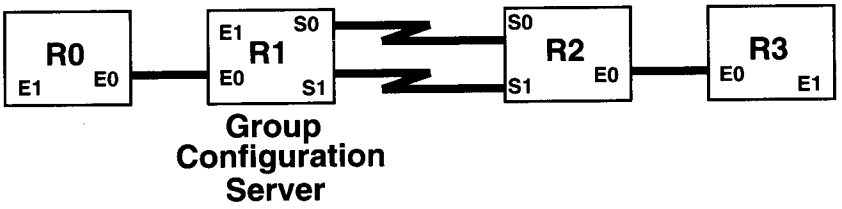
Verify that the startup-configuration downloaded properly.

Step 9 Repeat step 5 through step 8 for each of the startup-config files used for the other routers in your group.

Step 10 Set up the R1 router to be the group configuration server. Use the global config command **tftp flash** ***filename*** (where filename is a startup-config filename, for example, **seattle.icr**).

Repeat this command for each of the other downloaded router startup-config files.

Part 2: Use the group configuration server and TFTP copy the startup-config files.



Group Configuration Server Address:_____

Configuration Filename to TFTP Copy:_____

Step 1 On the R0, R2, and R3 routers, use the **telnet** or **show cdp neighbors detail** commands to obtain an address to use for R1.

Use **ping** to make sure that you can reach that address on the group configuration server.

Step 2 Use the **copy tftp startup-config** commandto start the download.

Step 3 When you see the prompt Address of remote host [255.255.255.255]?, enter the address of the group configuration server.

Step 4 When you see the prompt for Name of configuration file [*city-confg*]?, enter the filename of your startup-config file.

Step 5 Verify that the startup-configuration downloaded properly.

Step 6 Use **show startup-config** to verify that all startup-config files for the R0, R2, and R3 routers in the group contain the original configuration files.

Step 7 On the R1 router, use the command **copy tftp startup-config** to start the download.

When you see the prompt Address of remote host [255.255.255.255]?, enter the address of the classroom configuration server.

When you see the prompt for Name of configuration file [*city-confg*]?, enter the filename of your startup-config file.

Verify that the startup-configuration downloaded properly.

Step 8 When all the startup-config files are correct, restart the routers in the group with the **reload** command.

After the reload finishes, check the running configuration for your router. Then check that you can connect with all the other routers in your group.

Step 9 Tell your instructor when your group has reverted to the original configurations.

This final step of the lab completes the ICRC course. Congratulations!