Networking Concepts

This appendix describes concepts that can help you when designing your network and when configuring your router according to the examples in this guide.

This appendix contains the following sections:

- WAN Technologies
- CHAP and PAP Authentication
- Dialer Interfaces and Dialer Profiles
- Using Access Lists

WAN Technologies

This section describes the some of the WAN connection types that can be used with the Cisco 1700 router, such as ISDN, Frame Relay, and X.25.

ISDN

ISDN is a set of digital services that is available through your local telephone company. ISDN digitizes information that is sent over the telephone network so that voice, data, text, graphics, music, video, and other material can be sent over existing telephone wire.

ISDN Components

ISDN components include terminals, terminal adapters (TAs), network termination devices, line-termination equipment, and exchange-termination equipment.

ISDN Terminals

There are two type of ISDN terminals:

- Terminal equipment type 1 (TE1) is designed specifically to work with ISDN. TE1s connect to the ISDN network with 4-wire, twisted-pair cable.
- Terminal equipment type 2 (TE2) is non-ISDN equipment (such as DTE) that predates ISDN standards. TE2s connect to the ISDN network with a terminal adapter.

ISDN Network Termination Devices

Two types of ISDN terminal devices can connect your router to the telephone company conventional 2-wire local loop:

- Network termination type 1 (NT1)—In North America, the NT1 is provided by the customer. In most other parts of the world, the NT1 is part of the network provided by the ISDN service provider. WAN interface cards without an integrated NT1 need an external NT1 to connect to ISDN services. The Cisco 1604 and ISDN BRI U WAN interface card have an integrated NT1.
- Network termination type 2 (NT2)—This more complicated device is usually found in digital private branch exchanges (PBXs).

There is also a NT1/2 device that performs both the functions of an NT1 and an NT2.

Services

There are two types of ISDN services:

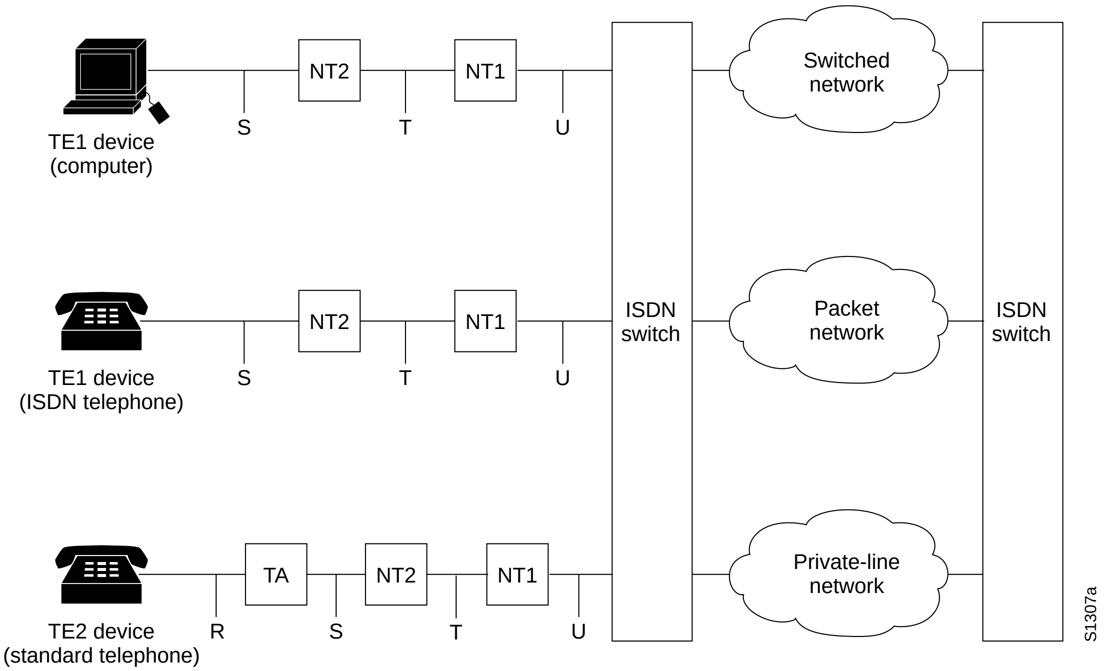
- Basic Rate Interface (BRI)—This service provides two B channels and one D channel. Each B channel operates at 64 kbps and carries user data. The D channel operates at 16 kbps and carries control and signaling information, although in certain circumstances it carries user data. BRI supports framing control and overhead, and the total bit rate is 192 kbps.
- Primary Rate Interface (PRI)—This service provides 23 B channels (which operate at 64 kbps) and 1 D channel (which operates at 64 kbps) in North America and Japan, resulting in a bit rate of 1.544 Mbps. In Europe, Australia, and other parts of the world, PRI provides 30 B channels, 1 D channel, and 1 maintenance/error channel. Each channel is 64 Kbps, for a total bit rate of 2.048 Mbps.

Sample Configuration

Figure A-1 shows an example ISDN configuration with the devices used to connect the user to the ISDN network.

Two of the devices shown, the computer and the ISDN telephone, are compatible with ISDN. The third device, the standard telephone, requires a TA to connect to the ISDN network through an NT2 or NT1 device.

Figure A-1 Sample ISDN Network



Frame Relay

Frame Relay is a method of packet-switching that is used for communication between user devices (such as routers, bridges, and host machines) and network devices (such as switching nodes and modems). User devices are called data terminal equipment (DTE), and network devices are called data circuit-terminating equipment (DCE).

Frame Relay services can be provided by either a public network or a network of privately owned equipment serving a single enterprise.

Frame Relay is a streamlined, efficient, high-performance protocol. It is extremely fast because

- It multiplexes many logical data conversations (or virtual circuits) over one physical link. Multiplexing provides flexible and efficient use of bandwidth.
- It uses fiber media/digital transmission links. These types of physical connections have a high level of data integrity, so Frame Relay does not need to perform error checking. Error checking is time-consuming and can decrease WAN performance.
- It does not need to perform flow control procedures because these types of procedures are done by upper-layer protocols. Frame Relay uses a simple congestion notification mechanism to inform user devices when the network become congested. Congestion notification alerts the higher-layer protocols that flow control is needed.

Current Frame Relay standards support permanent virtual circuits (PVCs) that are configured and managed in a Frame Relay network. The Cisco 1700 router supports switched virtual circuits (SVCs) for DTE interfaces.

Frame Relay also has Local Management Interface (LMI) extensions for supporting large, complex internetworks. Any LMI extension known as *common* should be implemented by anyone who supports the LMI specification. Other LMI extensions are known as *optional*.

The different LMI extensions are

- Virtual circuit status messages (common)—Provide communication and synchronization between the network and the user device, periodically report the existence of new PVCs and the deletion of existing PVCs, and provide information about PVC integrity.
- Multicasting (optional)—Allows a sender to transmit a single frame to multiple recipients, supporting the efficient routing of protocol messages and address resolution procedures that typically must be sent to many destinations simultaneously.
- Global addressing (optional)—Gives connection identifiers global rather than local significance, allowing them to be used to identify a specific interface to the Frame Relay network. Global addressing makes the Frame Relay network resemble a LAN in terms of addressing.

X.25

X.25 is a method of packet-switching that is used for communication between user devices (such as routers, bridges, and host machines) and network devices (such as switching nodes and modems). User devices are called data terminal equipment (DTE), and network devices are called data circuit-terminating equipment (DCE).

With X.25, one computer calls another to request a communication session. The called computer can accept or refuse the connection. If the call is accepted, the two computers begin full-duplex information transfer. Either computer can terminate the connection at any time.

User devices communicate with a bidirectional association called a *virtual circuit*. Devices on a network use virtual circuits to communicate through intermediate nodes without being directly, physically connected to each other. Virtual circuits are permanent or switched (temporary). Permanent virtual circuits (PVCs) are typically used for the most-often-used data transfers, and switched virtual circuits (SVCs) are used for sporadic data transfers.

Basic Rate Interface (BRI) is an ISDN interface consisting of two B channels (B1 and B2) and one D channel. The B channels are used to transfer data, voice, and video. The D channel carries signal and call setup information. IPX, AppleTalk, transparent bridging, XNS, DECnet, and IP can all be encapsulated as X.25 over the ISDN B channels.

ISDN uses the D channel to carry signal information. ISDN can also use the D channel in a BRI to carry X.25 packets. The D channel has a capacity of 16 kbps, and the X.25 over D channel can use up to 9.6 kbps.

You can set the parameters of the X.25-over-D-channel interface without disrupting the original ISDN interface configuration. In a normal ISDN BRI interface, the D and B channels are bundled together and represented as a single interface. The original BRI interface continues to represent the D, B1, and B2 channels.

Because some end-user equipment uses static terminal endpoint identifiers (TEIs) to access this feature, static TEIs are supported. The dialer recognizes the X.25-over-D-channel calls and initiates them on a new interface.

X.25 traffic over the D channel can be used as a primary interface where low-volume, sporadic interactive traffic is the normal mode of operation. Supported traffic includes IP, IPX, AppleTalk, and transparent bridging.

CHAP and PAP Authentication

When configuring your router, you must select a method of authentication. Authentication is used for security and to identify who is calling in so that the called router can correctly forward packets to the correct interface. This is generally required when using dialer rotary groups where multiple sites will be calling into a single router.

The example configurations in this guide use Point-to-Point Protocol (PPP) with Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) for security and authentication. CHAP and PAP, used with PPP encapsulation, allow routers to authenticate incoming calls.

CHAP Authentication

With CHAP, a remote device attempting to connect to the local router is requested, or challenged, to respond. When the local router receives the challenge response, it verifies the response by looking up the name of the remote device given in the response. The passwords must be identical on the remote device and the local router. The names and passwords are configured using the **username** command.

In the following example, Router Macbeth will allow Router Macduff to call in using the password “bubble”:

```
hostname Macbeth
username Macduff password bubble
!
encapsulation ppp
ppp authentication chap
```

In the following example, Router Macduff will allow Router Macbeth to call in using the password “bubble”:

```
hostname Macduff
username Macbeth password bubble
!
encapsulation ppp
ppp authentication chap
```

PAP Authentication

Like CHAP, PAP is an authentication protocol used with PPP. However, PAP is less secure. CHAP passes an encrypted version of the password on the physical link, but PAP passes the password and hostname or username in clear text.

When using interactive mode (rather than dedicated mode) on asynchronous lines, the **username** command allows a router to verify a username in an internal database before the user can call in to the router. In the following example, user Joe Smith will be allowed to call in to the router if he uses the password “freedom”:

```
username JoeSmith password freedom
line 1
login
```

Using Access Lists

This section is a general description of access lists. Because access lists affect network security, you should understand how they work before using them in your network. For detailed information on how access lists work and how to configure them, refer to the "Configuring IP Services" chapter in the *Network Protocols Configuration Guide, Part 1* publication, which is available on the Documentation CD-ROM that came with your router.

Access lists control packet filtering on Cisco routers by limiting traffic and restricting network use by certain users or devices. Although there are several purposes for using access lists, the example configurations in this guide use access lists to control the transmission of packets on a specific interface.

An access list is a sequential collection of permit and deny conditions that apply to network addresses. Packet addresses are compared to the conditions in all access lists configured in the router. The first match determines whether or not the packet is accepted or denied by the router. Because the router stops testing conditions after the first match, the order in which the conditions are defined in the access list is critical. If a packet does not match any conditions configured in an access list, the router rejects the packet.

Dialer Interfaces and Dialer Profiles

A dialer interface is a WAN interface on the router that is not connected to a remote device all the time, but dials the remote device whenever a connection is required. Configuring an interface on a Cisco router to dial a specific remote device at specific times requires configuring dialer profiles.

You can use dialer profiles to configure the router physical interfaces separately from the logical configuration required for a call. You can also configure the router to allow the logical and physical configurations to be dynamically bound together on a per-call basis. All calls going to or from the same destination subnetwork use the same dialer profile.

A *dialer profile* consists of the following elements:

- A *dialer interface* (a logical entity) configuration with one or more dial strings, each used to reach a specific destination subnetwork.
- A *dialer map class* defining all the characteristics for any call to the specified dial string (telephone number).
- An *dialer pool* of physical interfaces to be used by the dialer interface. The physical interfaces in a dialer pool are ordered according to priority.

Dialer Interfaces

A dialer interface configuration is a group of settings the routers uses to connect to a remote network. One dialer interface can use multiple dial strings (telephone numbers). Each dial string is associated with its own dialer map class. The dialer map class defines all the characteristics for any call to the specified dial string. For example, the dialer map class for one destination might specify a 56-kbps ISDN speed, and the map class for a different destination might specify a 64-kbps ISDN speed.

Dialer Pools

Each dialer interface uses one group of physical interfaces called a dialer pool. The physical interfaces in a dialer pool are ordered based on priority. One physical interface can belong to multiple dialer pools. ISDN BRI interfaces can set a limit on the minimum and maximum number of B channels reserved by any dialer pools. A channel reserved by a dialer pool remains idle until traffic is directed to the pool.

When you use dialer profiles to configure dial-on-demand routing (DDR), the physical interface is configured only for encapsulation and the dialer pools that the interface belongs to. All other characteristics used for making calls are defined in the dialer map.