CHAPTER 1

WAN Technologies and Components

Over the last several years, web-based applications, wireless devices, and virtual private networking (VPN) have changed our expectations about computer networks. Today's corporate networks are accessible virtually anytime from anywhere, with many users expecting access to their company's network while at home or on the road.

Corporate networks are typically built around one central site that houses key network resources. These resources include file servers, web servers, and e-mail servers that deliver information and services to all users in a company. Such services are readily accessible to central site users through their LAN but how will users working remotely gain access to these resources?

As a networking professional, it is your job to provide users with secure remote access to the network. Remote users might be working at branch offices or home offices, or they might even be on the road with a laptop or a handheld mobile device. Essentially, a remote user is any user who is not presently working at the company's central site.

Remote access solutions come in all shapes and sizes. Each company's solution typically involves a combination of varied WAN services. Most of these services are obtained from a service provider, such as a regional telecommunications company. Because the transmission facilities belong to a service provider, your role is to select the appropriate service, not actually to design and maintain the WAN facilities themselves.

Types of available WAN services and their costs vary depending on geographical region and the provider. Real-world budgetary constraints and service availability are often the overriding selection criteria.

To implement the most appropriate solution, you must understand the advantages and disadvantages of the different types of WAN services.

This chapter discusses various remote access technologies and considerations facing an enterprise when building its corporate network. This chapter also addresses Cisco product selection information.

WAN Connection Characteristics

Many significant WAN connection characteristics can be grouped into the following categories:

- Connection duration

  Dedicated

  — Always on.

  — Cost is typically related to bandwidth and distance.

  On demand

  — Connected on demand.

  — Cost related to time of usage and bandwidth and distance.

- Switching

  Circuit switched

  — End-to-end bandwidth allocation and control.

  — Provisioned permanently or on demand.

  Packet switched

  — Asynchronous Transport Network (ATM).

  — Statistical bandwidth allocation in transport network.

  — Cost typically related to bandwidth guarantee and other quality of service (QoS) parameters.

- Synchronization mechanism

  External

  — Clocking determined by a separate conductor in the media.

  — Thicker cable with more conductors per connection.

  Embedded

  — Clocking determined by bit times within the data stream.

  — Fewer conductors per connection.

- Data rate

  Narrowband

  — Rates up to and including 128 kbps (Example: dialup).

  Broadband

  — Data rates greater than narrowband rates. (The exact dividing line involves more marketing than technology. Broadband is greater than *ISDN* Basic Rate Interface [BRI] and equal to or less than T3 line example: cable modem.)

- Termination

  End-to-end circuits

  — Bit synchronization and data link termination is managed at the ends of the circuit, giving an appearance of increased control. The service provider is transparent.

  Transport network

  — The intermediate network terminates bit synchronization; content is carried asynchronously across the transport network. Includes packet switching Frame Relay (FR) and ATM and broadband access technologies.

- Transmission media

  Copper: Cheaper for lower data rates and shorter distances

  — Twisted pair.

  — Coaxial cable.

  Fiber: Carrier for high data rates and longer distances

- Multimode.
- Single mode.

Table 1-1 provides a list and comparison of various WAN connection characteristics.

Table 1-1 *WAN Connection Characteristics*

Connection Duration	**Dedicated**	**On Demand**
Switching	Circuit	Packet
Synchronization	External	Embedded
Data Rate	Narrowband	Broadband
Termination	End-to-end	Transport network
Media	Copper - Twisted pair - Coaxial	Fiber - Multimode - Single mode

Common WAN Connection Types

For the purpose of this discussion, WAN connections have been grouped in four general categories, which reflect generally available WAN services:

- Dedicated circuited switched
- On-Demand circuit switched
- Packet-switched virtual circuit
- Broadband access

Dedicated Circuit Switched-Connections

Leased line serial connections typically connect to a transport service provider through a *data communications equipment (DCE)* device, which both provides a clock and transforms the signal to the channelized format used in the service provider network. These point-to-point dedicated links provide a single, pre-established WAN communications path from the customer premises, circuit switched through a carrier network, to a remote network. Dedicated lines through T3/E3 rates are frequently described as leased lines. The established path is permanent and fixed for each remote network reached through the carrier facilities. The service provider reserves the private use of the customer circuits through the transport network full time.

Synchronization of the timing and data-link control is preserved end to end. These dedicated connections are made using the synchronous serial ports on the router with bandwidth use of up to 34 Mbps over a service provider E3 transport link and 45 Mbps over T3. Different encapsulation methods at the data link layer provide flexibility and reliability for user traffic. Typical connections on a dedicated network WAN connection employ 56 kbps, 64 kbps, T1, E1, T3, and E3 data rates.

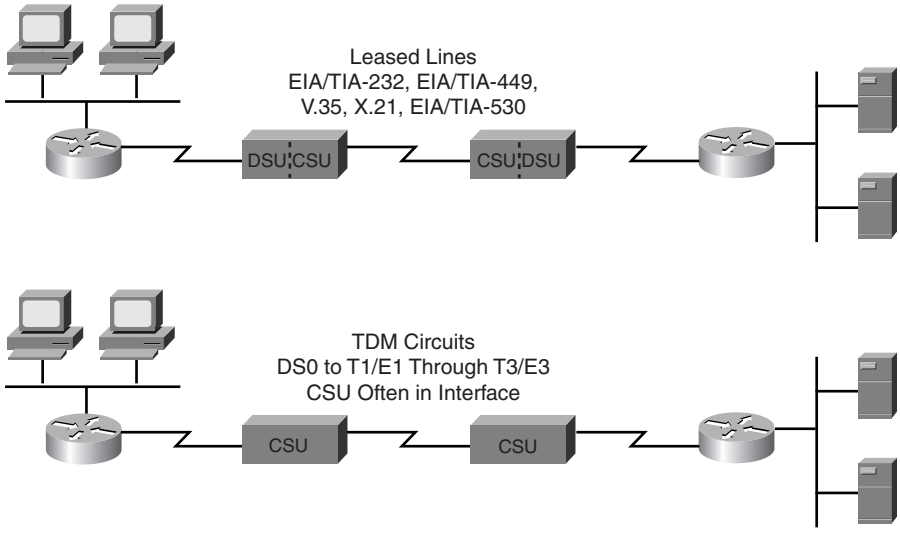
The following synchronous serial standards are supported on Cisco routers through serial interfaces:

- Electronic Industries Association/Telecommunications Industry Association (EIA/TIA)-232
- EIA/TIA-449
- V.35 (48 kbps)
- EIA/TIA-530
- X.21 (2 Mbps)

In North America the connecting device is called a *channel service unit/data service unit (CSU/DSU)*, as shown in Figure 1-1. The CSU connects to the service provider network, while the DSU connects to the network device serial interface. It is a device (or sometimes two separate digital devices) that adapts the media format from a serial data terminal equipment (DTE) device, such as a router, to the media format of the service provider equipment, such as a WAN switch, in a switched carrier network. The CSU/DSU also provides signal clocking for synchronization between these devices. Figure 1-1 shows the placement of the CSU/DSU.

It is increasingly common to have direct connections to the carrier transport network using fractional or complete T1/E1 circuits. In this case, a CSU provides demarcation and logical termination between the service provider network and the customer network. Direct T3/E3 and SONET/SDH (Synchronous Optical NETwork/Synchronous Digital Hierarchy) connectivity might also be available for organizations requiring higher data rates.

Figure 1-1 *Dedicated Circuit-Switched-Connections*



The private nature of a dedicated connection allows a corporation better control over the WAN connection. Dedicated connections also offer high speeds beyond T3/E3 levels using SONET/SDH. Dedicated connections are ideal for high-volume environments with steady-rate traffic patterns or high peak demands of critical traffic. However, because the line is not shared, dedicated connections tend to be more costly.

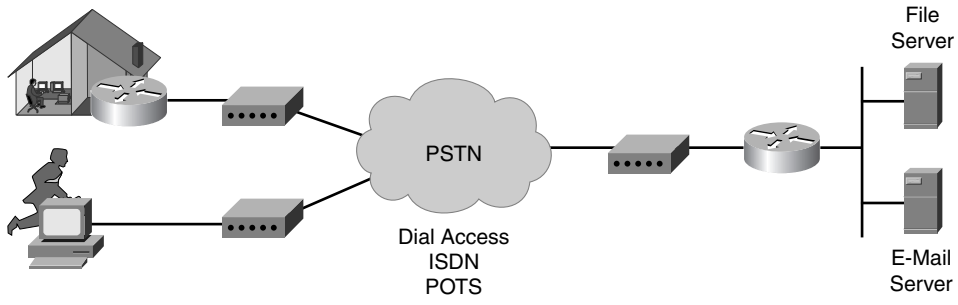
As a general rule, dedicated connections are most cost-effective in the following situations:

- Long connect times
- Short distances
- Critical traffic requirements that *must* be guaranteed

On-Demand Circuit-Switched Connections

On-demand circuit switching is a WAN transport method in which a dedicated physical circuit through a Public Switched Telephone Network (PSTN) is established, maintained, and terminated for each communication session, as shown in Figure 1-2. Initial signaling at the setup stage determines the endpoints and the connection between the two endpoints.

Figure 1-2 *On-Demand Circuit-Switched Connections*



Typical circuit-switched connections are as follows:

- Asynchronous modem
- ISDN Basic Rate Interface (BRI) and ISDN Primary Rate Interface (PRI)

Advantages of on-demand connection types include dynamic selection of the circuit endpoint, and the accumulation of charges for transport while only connections are active. Costs are directly related to connection time and distance for each POTS line or ISDN bearer channel. As traffic between endpoints increases in volume, the duration of the connection increases.

Asynchronous Modem Connections

Asynchronous modem connections require minimal equipment cost and use the existing telephone network. Users can easily access a central site from any location that has a telephone connection into a telephone network.

The nature of asynchronous connections allows you to configure your connection to be enabled only when you need the service by using dial-on-demand routing (DDR) through the modem using an asynchronous serial interface. DDR is ideal when you need only short-term access.

Enable DDR on your asynchronous interface when the following is true:

- **Traffic patterns are low-volume or periodic**—Calls are placed and connections are established only when the router detects traffic marked as "interesting." Periodic broadcasts, such as routing protocol updates, should be prevented from triggering a call.
- **You need a backup connection for redundancy or load sharing**—DDR can be used to provide backup load sharing and interface failure backup.

A router acts as a network access server, which is a concentration point for dial-in and dial-out calls. Mobile users, for example, can call in to an access server at a central site to access their e-mail messages.

Asynchronous connections are useful in the following situations:

- A backup connection is required.
- You have a small site.
- Short-term on-demand access is needed.
- Periods of lower network traffic and fewer users. Depending on network size, this number is generally 18 percent or below. This percentage has become a practical, low-volume standard in networks at most organizations.

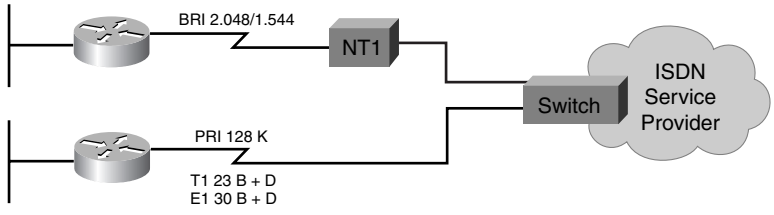
Asynchronous connections through the PSTN require modems at each end of the connection to convert digital data signals to analog signals that can be transported over the telephone network. Modem speeds typically vary from 19.2 kbps to 56 kbps depending on line quality. The slower bandwidth speeds limit the amount of traffic you might want to send over an asynchronous line. To place or receive an asynchronous serial call, set up a Cisco router with an asynchronous serial interface. The serial standard to attach to an external modem is EIA/TIA-232. The interface to the telephone company varies by country. In the United States, a standard RJ-11 adapter connects the modem to the telephone outlet.

ISDN Connections

Integrated Services Digital Network (ISDN) connections are typically switched connections that, like asynchronous connections, provide WAN access when needed rather than requiring a dedicated link. ISDN offers increased bandwidth over a typical dial-up connection, faster setup, and is intended to carry data, voice, and video traffic across a telephone network.

To place an ISDN BRI call, you should set up your router with a BRI interface, as shown in Figure 1-3, or an ISDN terminal adapter, which is a device used to connect ISDN BRI connections to other interfaces such as EIA/TIA-232. A terminal adapter is essentially an ISDN modem. You should also consult your telephone company for information specific to your connection.

Figure 1-3 *ISDN Connections*



NOTE Generally, in Europe, the service provider supplies the Network Termination 1 (NT-1). In North America, the customer supplies the NT-1.

ISDN PRI is configured over connections such as T1 and E1 technologies. T1 is used in North America, and E1 is common in other countries. To place an ISDN call, set up your router with the proper connection.

As with asynchronous connections, you can also configure DDR to control access for specific periods of time.

Packet-Switched Virtual Connections

Packet switching is a method in which a network device uses a single point-to-point link to a service provider to transport packets intended for one or more destinations across a carrier network, as shown in Figure 1-4. Packet switching is a networking technology based on the transmission of data in packets. Dividing a continuous stream of data into small units (packets) enables data from one or more sources to one or more destinations to share the communication channels within the transport network.

Figure 1-4 *Packet-Switched Connections*

- Virtual circuits are established.
- Packet-switched networks generally share bandwidth statistically.

Packet-switched networks use virtual circuits (VCs) that provide end-to-end connectivity. Statically programmed switching devices accomplish physical connections. Packet headers identify the circuit, and the headers might change on each network link traversed. It requires the use of precise switching information throughout the transport network.

Packet-switched networks can be either privately or publicly managed. The underlying switching fabric is transparent to the network user, and the switches are responsible for only the internal delivery of data across the packet-switched network. Packet switching is implemented at the data link layer of the ISO/OSI reference model. Various packet-switching technologies are more fully discussed in subsequent chapters.

Packet-switched networks offer an administrator less control than a point-to-point connection, and the bandwidth is shared statistically. However, the cost is generally less than a leased line. With WAN speeds comparable to those of leased lines, packet-switched networks are generally suitable for links between two large sites that require high link utilization or present high peaks of critical traffic.

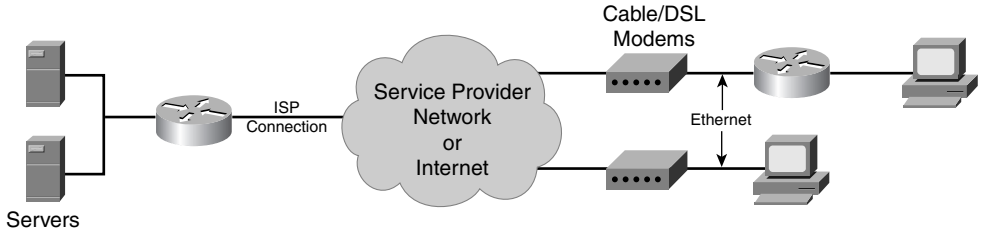
As a general rule, packet-switched connections are most cost-effective in the following situations:

- Long connect times
- Large geographic distances
- High link utilization
- High peaks of critical traffic

Broadband Access

Internet access is moving from dial-up modems and slow connections to broadband access using a variety of technologies that take advantage of existing telephone and cable television distribution infrastructures to provide broadband access to the Internet, as shown in Figure 1-5. Examples of this include DSL and high-speed cable broadband technologies. Broadband is generally defined as any sustained data rate above 128 kbps. Broadband can allow remote office staff and small office/home offices (SOHOs) to connect to the central site at higher data rates than traditional on-demand technologies.

Figure 1-5 *Broadband Access*



High-speed broadband access to the Internet through a broadband point of presence (POP) and then to corporate networks using secure virtual private networks (VPNs) is a reality for many users in the networked world today. This broadband access has the potential to directly improve employee productivity and to provide a foundation for new voice and video business services over the Internet.

Many corporations and educational institutions have implemented broadband access solutions for access by suppliers, customers, and staff. The use of the Internet for secure site-to-site connectivity using VPNs is increasing, especially for these types of connections and subsequent traffic.

Broadband access technology options include cable modems and various forms of DLS technology including Asymmetrical DSL (ADSL), ISDN DSL (IDSL), Symmetrical DSL (SDSL), and High-Data-Rate DSL (HDSL). The most common problem in offering these broadband services to remote users is lack of availability of the cable modem and/or DSL services in the user's local area due to infrastructure deficiencies.

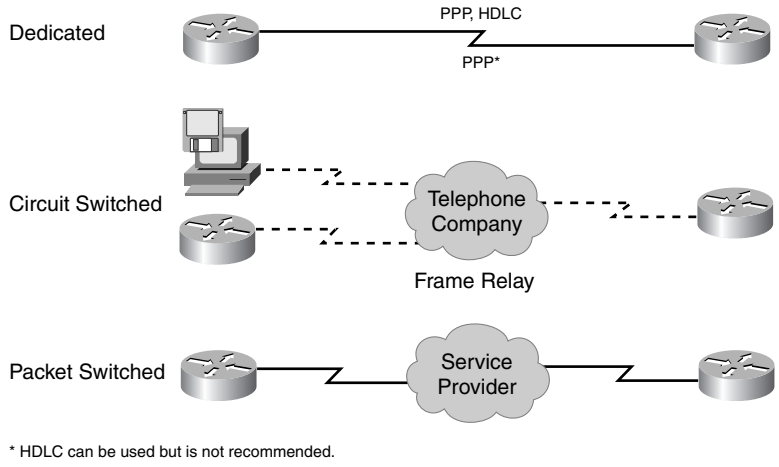
Defining WAN Encapsulation Protocols

Each WAN connection uses a Layer 2 protocol to encapsulate the network traffic while it is crossing the WAN link. To ensure that the correct encapsulation protocol is used, you need to configure the Layer 2 encapsulation type to use. The choice of encapsulation protocol depends on the WAN technology and the communicating equipment. Typical WAN protocols include the following and are shown in Figure 1-6:

- **Point-to-Point Protocol (PPP)**—PPP (PPPoE, PPPoA) originally emerged as an encapsulation protocol for transporting IP traffic over point-to-point links. PPP also established a standard for the assignment and management of IP addresses, asynchronous (start/stop) and bit-oriented synchronous encapsulation, network protocol multiplexing, link configuration, link-quality testing, error detection, and option negotiation for such capabilities as network layer address negotiation and data-compression negotiation. PPP supports these functions by providing an extensible Link Control Protocol (LCP) and a family of Network Control Protocols (NCPs) to negotiate optional configuration parameters and facilities. The broadband connection type used determine the use of Point-to-Point Protocol over Ethernet (PPPoE) or Point-to-Point Protocol over ATM (PPPoA).
- **High-Level Data Link Control (HDLC)**—HDLC is the default encapsulation type on Cisco synchronous serial interfaces. It is a bit-oriented synchronous data link layer protocol. HDLC specifies a data encapsulation method on synchronous serial links using frame characters and checksums. HDLC is a standard that is open for interpretation. As a result, there are different versions of HDLC. If communicating with a non-Cisco device, synchronous PPP is a more viable option.
- **Frame Relay**—High-performance packet-switched WAN protocol that operates at the physical and data link layers of the OSI reference model. Frame Relay was designed originally for use across ISDN interfaces. Today, it is used over a variety of other network interfaces and typically operates over WAN facilities that offer more reliable connection services and a higher degree of reliability.

- **Asynchronous Transfer Mode (ATM)**—ATM is the international standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53-byte) cells. Fixed-length cells allow processing to occur in hardware, thereby reducing transit delays. ATM is designed to take advantage of high-speed transmission media such as E3, SONET, and T3, or any transmission media up to 10 Gbps.

Figure 1-6 *WAN Protocols*



PPP Encapsulation

PPP is an international standard encapsulation used for the following types of connections:

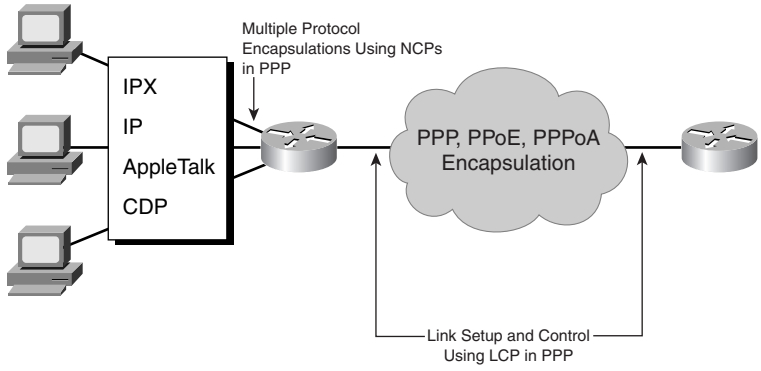
- Asynchronous serial
- ISDN
- Synchronous serial
- Broadband

PPP (RFC 1331: http://www.faqs.org/rfcs/rfc1331.html) provides a standard method of encapsulating higher-layer protocols across point-to-point connections. PPP extends the HDLC packet structure with a 16-bit protocol identifier, which contains information about the content of the packet.

Because it is standardized, PPP supports vendor interoperability.

PPP uses its NCP component to encapsulate multiple protocols. Figure 1-7 shows an example of PPP encapsulation.

Figure 1-7 *PPP Encapsulation*



PPP uses another of its major components, the LCP, to negotiate and setup control options on the WAN data link. More LCP options are discussed in Chapter 4, "Configuring PPP and Controlling Network Access with PAP and CHAP"; however, some of the PPP LCP features covered here include the following:

- **Authentication**—The process of identifying an individual, usually based on a username and password
- **Compression**—Storing data in a format that requires less space than usual.
- **Multilink**—An extension to the PPP protocol that allows multiple physical connections between two points to be combined into a single logical connection.

PPPoE, which is referenced in RFC 2516, provides the ability to connect a network of hosts over a simple bridging access device to an access concentrator. With this model, a host utilizes its own PPP stack and the user is presented with a familiar user interface. Access control, billing, and type of service can be done on a per-user, rather than a per-site, basis.

PPPoA was primarily implemented as part of an ADSL. It relies on RFC 1483, now RFC 2686, operating in either LLC-SNAP or VC-Mux mode. Customer premises equipment (CPE) encapsulates PPP sessions based on this RFC for transport across the ADSL loop and the digital subscriber line access multiplexer (DSLAM).

In these architectures, IP address allocation is based on IP Control Protocol (IPCP) negotiation, the same principle of PPP in dial mode.

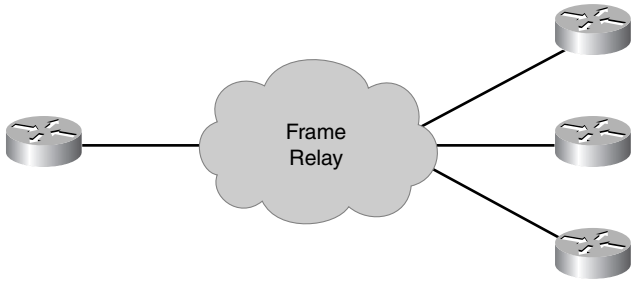
In PPPoE, the source of IP address allocation depends on the type of service to which the subscriber has subscribed and where the PPP sessions are terminated. PPPoE makes use of the dialup networking feature of Microsoft Windows, and the IP address assigned is reflected within the PPP adapter. PPPoE can be used on existing CPE (which cannot be upgraded to PPP or which does not have the capability to run PPPoA), extending the PPP session over the bridged Ethernet LAN to the PC. PPPoE can also be configured on the CPE to terminate the PPP session and use Network Address Translation (NAT) for workstation access to the Internet.

PPPoA requires no host-based software, only that each CPE device must have a username and password for authentication to a central site. The PPP sessions initiated by the subscriber are terminated at the service provider that authenticates users via a local database through a RADIUS or TACACS+ server. The PPPoA session authentication is based on Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). The service provider only needs to assign one IP address for CPE, and the CPE can be configured for NAT.

Frame Relay Encapsulations

Frame Relay is an industry-standard data link layer protocol commonly used in packet-switched networks. Frame Relay supports technological advances such as fiber-optic cabling and digital transmission. Frame Relay can eliminate time-consuming processes (such as error correction and flow control) that are necessary when using older, less-reliable WAN media and protocols. Figure 1-8 shows an example of a Frame Relay Encapsulation topology.

Figure 1-8 *Frame Relay Encapsulation*



When purchasing bandwidth, customers buy a committed information rate (CIR) from the carrier to ensure their minimum bandwidth requirements are met. Adding an additional channel or data-link connection identifier (DLCI) provisions a new VC and set of connection characteristics. Adding more DSs (channels) to an existing DLCI (should the physical facilities support it) adds bandwidth. Channels can be easily added in this manner to meet growth requirements.

Because of the use of a public network, a service provider must be consulted to obtain information specific to a link.

Determining the WAN Types to Use

When you design internetworks, you must make several key decisions concerning connectivity between different users or groups of users in your WAN environment. Some of these decisions include security, availability, or bandwidth, for example.

When selecting a WAN connection, you should also consider the following:

- **Availability**—Each method of connectivity has characteristics inherent in its design, usage, and implementation. For example, Frame Relay is not available in all geographic regions.
- **Bandwidth**—WAN bandwidth is expensive, and organizations cannot afford to pay for more bandwidth than they need. Determining usage over the WAN is a necessary step toward evaluating the most cost-effective WAN services for your needs.
- **Cost**—WAN usage costs are typically 80 percent of the entire information services budget. Cost is a major consideration when different WAN services and different service providers are evaluated. If, for example, you use the line for only 1 hour a day, you might want to select a dial-on-demand connection such as an asynchronous or ISDN connection.
- **Ease of management**—Network designers are often concerned about the degree of difficulty associated with managing connections. Connection management includes both the configuration at initial startup and the outgoing configuration tasks of normal operation. Traffic management is the capability of the connection to adjust to different rates of traffic regardless of whether the traffic is steady state or bursty in nature. Dedicated lines are often easier to manage than shared lines.
- **Application traffic**—The application traffic might be many small packets, such as a terminal session, or very large packets, such as during file transfer.
- **QoS and reliability**—How critical is the traffic intended to travel over the link? A backup connection might be necessary.
- **Access control**—A dedicated connection might help control access, but electronic commerce cannot occur on a wide scale unless consumers can access some portion of your network.
- **QoS**—QoS is a major concern to network administrators these days, because companies are not spending as much on WAN costs and are being smarter and trying to get the most out of what they have.

WAN Connection Speed Comparison

Figure 1-9 illustrates the WAN speeds for typical technologies. In this example, a network administrator must select a WAN option, based on the amount of required bandwidth.

The speeds, costs, and availability of WANs vary internationally. For example, in North America, high-bandwidth speeds such as T1 are readily available at reasonable prices.

Europe offers comparable speeds such as E1, but the prices tend to be higher. Other parts of the world offer limited WAN services with lower bandwidth speeds, typically up to 64 kbps, and the costs are higher. Broadband options include DSL and high-speed cable modems.

Broadband is generally defined as any sustained speed above 128 kbps, but that might soon be changing. Broadband can allow remote office staff and SOHOs to connect to the central office LAN at high speeds.

A cable modem can provide up to 90 times the speed (4 Mbps) of a dialup connection for remote access.

DSL is a technology that enables the use of unused bandwidth that already exists on a regular phone line to deliver fast digital data transmission up to 25 times the speed (approximately 1 Mbps) of a dialup connection without affecting the analog telephone service used.

Figure 1-9 *WAN Connection Speed Comparison*

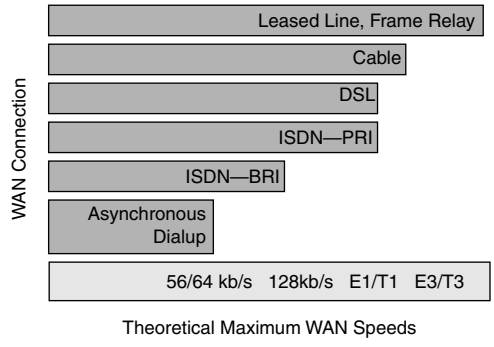


Table 1-2 compares considerations for various types of WAN connections. Each WAN connection has advantages and disadvantages. For example, setting up a dialup asynchronous connection offers only limited bandwidth, but a user can call in to the office from anywhere over the existing telephone network.

Table 1-2 *WAN Connection Summary*

Connection Type	Attributes
Leased Line	High control, full-bandwidth, high-cost enterprise networks, and last-mile access
Broadband	Cable—A very fast connection shared through a LAN to the Internet. Low cost, but performance can vary.
	DSL—Converts existing phone lines into access paths for multimedia and high-speed data transfers. Most high-performance DSL connections have distance limitations.

continues

Table 1-2 *WAN Connection Summary (Continued)*

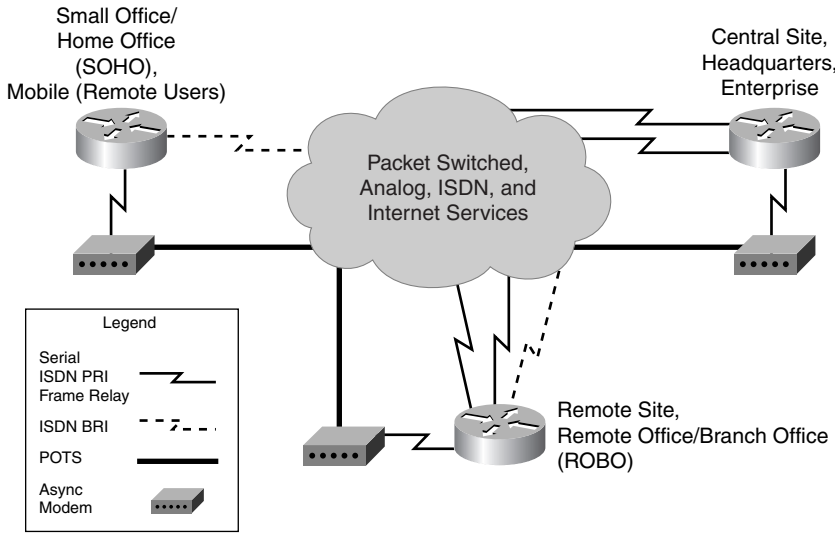
Connection Type	Attributes
ISDN	Creates a digital loop. Higher bandwidth than typical dialup, often with higher cost.
Analog	Slow setup and transmission speeds. Location flexibility.

Identifying Site Requirements

A company might have multiple sites that vary in size. A remote network is necessary to connect the various locations in a company. Typical site locations shown in Figure 1-10 include the following:

- **Central site**—The central site is a large company site that is often the corporate headquarters or a major office. This is the site that other regional and branch offices and SOHOs can connect to for data and information services. Because users might access this site via multiple WAN technologies, it is important to design your central site to accommodate many different types of WAN connections from remote locations. The central site is often called headquarters, the enterprise, or corporate.
- **Remote site**—The remote site is a smaller office that generally accommodates employees who have a compelling reason to be located in a specific region, such as a regional salesperson. Remote site users must be able to connect to the central site to access company information. Remote sites are sometimes called branch offices, remote office/branch offices (ROBOs), or sales offices. Small and medium-sized businesses can benefit from high-speed Internet access, VPN connectivity to corporate intranets, telecommuting capabilities for work-at-home employees, interactive television, and economical PSTN for quality voice over IP. Large and small businesses have employees who work from their homes. To stay in touch, they need secure, high-speed, remote access to the corporate intranet and access to the Internet for e-mail communication with customers and suppliers.
- **SOHO site**—This is a small office with one to a few employees, or a home office of a telecommuter. Depending on the amount of use and the WAN services available, telecommuters tend to use dialup and broadband services. Telecommuters can also be mobile users who travel. Mobile users are specific telecommuters who do not work at a fixed company site. Because their locations vary, mobile users tend to access the company network via an asynchronous dialup connection through the telephone company or they might lock onto the corporate intranet using VPN client software on their laptops. Telecommuters, working out of their home, can also use a VPN tunnel gateway router for all encrypted data and voice traffic from the company intranet. These solutions provide the enterprise professional, simple, and safe access for branch offices or SOHOs to access the corporate network site, depending on the needs of users at the sites.

Figure 1-10 *Company Site*



Central Site Considerations

The central site WAN connection is a critical focal point for a company. Other sites and users access this site for information and, typically, these remote sites do not communicate together because they only connect to the hub or central site. Because many users access this site in a variety of ways, it is important that your central site solution has a modular design that can accommodate many different types of WAN connections from remote locations.

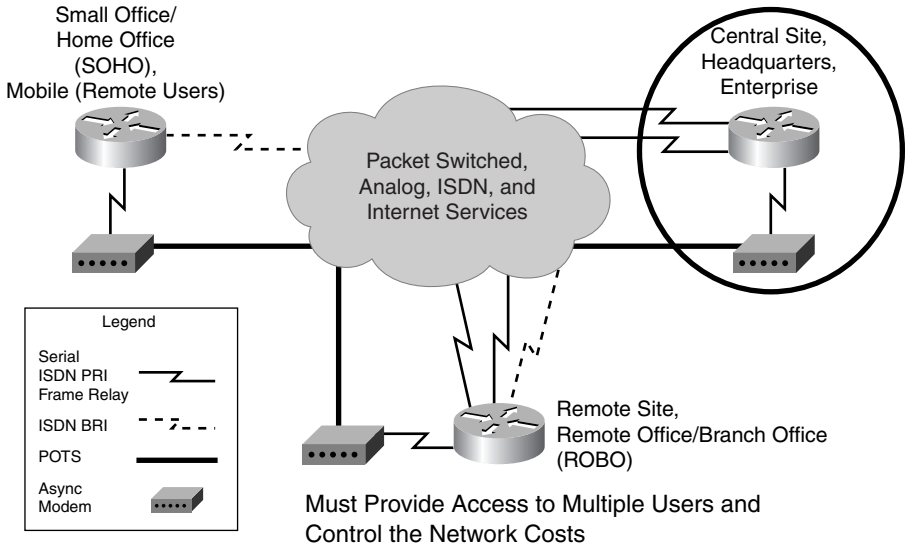
The technologies and features used to connect company campuses over a WAN are developed to optimize the WAN bandwidth, minimize the cost, and maximize the effective service to the end users. You should choose the WAN architecture that provides the most cost-effective bandwidth and a technology that optimizes service to the end users. With that in mind, central site considerations include the following, further illustrated in Figure 1-11:

- **Multiple access connections**—Users connect to the central site using different media. Central site considerations must include multiple media options and simultaneous access from multiple users.
- **Cost**—Keep the costs low while maintaining a satisfactory level of service. For example, because some WAN charges are based on usage, such as ISDN, it is important that companies have a solution that can implement features to optimize bandwidth and minimize WAN costs. Features such as DDR and compression ensure that WAN costs are kept to a minimum. In another example, because leased lines are

generally charged on a fixed basis, you might want to consider this service only if the line can sustain a certain link utilization level. Broadband connections such as cable and DSL offer a low-cost, high-speed solution.

- **Access control**—Company information must be restricted, allowing users access only to areas in the network for which they are authorized. For example, access lists can filter out unauthorized data flow between offices. PPP network links, such as PAP and CHAP, can identify the remote entity to prevent unauthorized network connection. SOHOs and branch office users gain access to secure sites through the use of VPN technologies. (These technologies are discussed in depth in Chapter 12, "Virtual Private Networks.")
- **QoS**—It is important to prioritize traffic over the link and manage traffic flow so that bursty traffic does not slow mission-critical traffic.
- **Redundancy and backup**—Because a link can fail or high link utilization can occur at certain peak usage times during the day, it is important to back up the connection to the central office (CO), for example. Avoid backing up links using the same service provider.
- **Scalability**—Build a network that can grow with the company.

Figure 1-11 *Central Site*



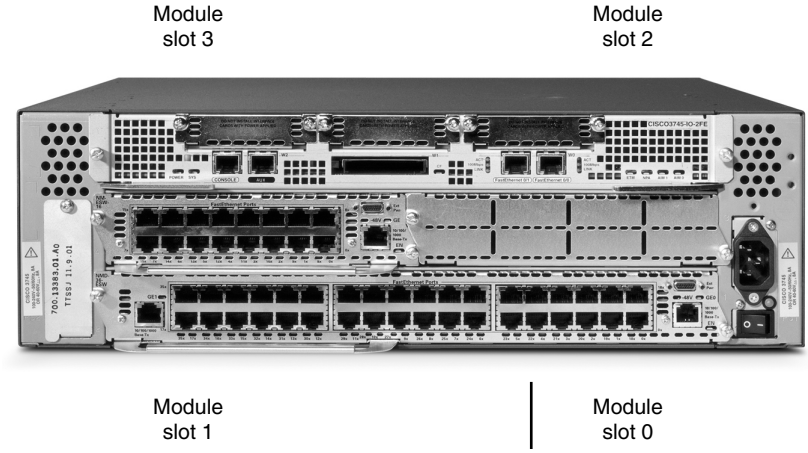
Central Site Router Equipment

Choose the router that supports the WAN protocols you use. As illustrated in Figure 1-11, the router and network modules support the interfaces in the network topology.

The following routers are typical Cisco solutions for a central site shown in Figure 1-12:

- Cisco 2600 series
- Cisco 3600 series
- Cisco 3700 series
- Cisco 4000 series
- Cisco 7200/7500 series

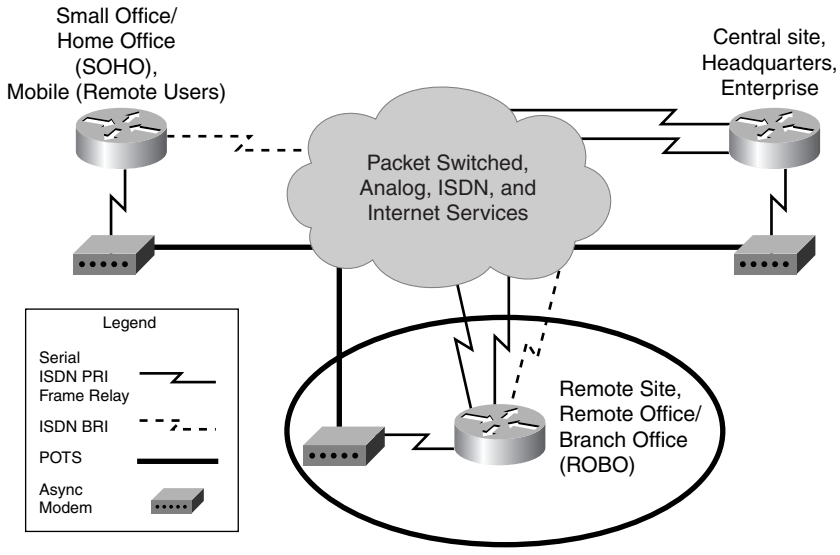
Figure 1-12 *Central Site Router Equipment*



Remote/Branch Office Considerations

A remote site, or branch office, is a smaller site connection to a central site over a WAN. A remote site typically has fewer users than the central site and, therefore, needs a smaller-size WAN connection (see Figure 1-13).

Figure 1-13 *Branch Office Considerations*



Remote sites connect to the central site and to some other remote site offices. Telecommuters might also require access to the remote site. A remote site can use the same or different media to connect to another remote site as they would to connect to the central site.

Remote site traffic can vary, but is typically sporadic. The network designer must determine whether it is more cost effective to offer a permanent or dialup solution.

The remote site must have a variety of equipment, but not as much as the central site requires. Typical WAN solutions a remote site uses to connect to the central site follow:

- Leased line
- Frame Relay
- ISDN
- Broadband services (cable or DSL)

Typical considerations for a remote site WAN connection follow:

- **Multiple access connections**—A connection is defined as multiple access when you have a line or channel and a device connecting three or more different service points. A concentrator connects all end stations in the network. Multiple access connections provide an interface between these devices and the network interface of a router.

- **Cost**—The cost is sometimes called path cost. This is an arbitrary value, typically based on hop count, media bandwidth, or other measures, that is assigned by a network administrator and used to compare various paths through an internetwork environment. Routing protocols use cost values to determine the most favorable path to a particular destination: The lower the cost, the better the path.
- **Access control**—To prevent unauthorized traffic, routers and firewalls use a set of rules that permit or deny certain traffic. Access control is commonly applied to router interfaces, and can be configured to control which data sessions can pass and which fail. Users can gain secure access by using VPN solutions to connect to corporate intranets.
- **Redundancy**—In internetworking, duplicate devices, services, or connections can perform the work of original devices, services, or connections in the event of a failure. Redundancy is the portion of the total information contained in a message that can be eliminated without loss of essential information or meaning.
- **Authentication**—The remote site must be able to authenticate itself to the central site.
- **Availability**—Service providers might not offer certain WAN services in some regions. This consideration generally becomes more critical as sites are set up in more remote locations.

Branch Office Router Equipment

Choose the router that supports the WAN protocols and interfaces you use. As illustrated in Figure 1-13, the 1700 series router and the respective WAN interface card (WIC) is an example of a branch office router that supports the interfaces required in the network topology. Figure 1-14 shows typical branch office router equipment.

The following routers are typical Cisco solutions for a branch office:

- Cisco 1600 series
- Cisco 1700 series
- Cisco 2500 series
- Cisco 2600 series
- Cisco 3600 series

Figure 1-14 *Branch Office Router Equipment*

1721 Router—Front View

ISDN WIC
1BU Card

1721 Router—Rear View

Serial WAN
Interface Card

SOHO Site Considerations

Improvements in WAN technologies allow many employees to do their jobs almost anywhere. The growth in the number of SOHO and small company sites has exploded. Like that of central and remote sites, the SOHO site must determine its WAN solution by weighing cost and bandwidth requirements.

An asynchronous dialup solution using the existing telephony network and an analog modem is often the solution for SOHOs because it is easy to set up and the telephone facilities are already installed. As usage and bandwidth requirements increase, other remote access technologies should be considered.

The nonstationary characteristics of a mobile user make an asynchronous dialup connection the remote solution. Employees on the road can use their PCs with modems and the existing telephone network to connect to the company.

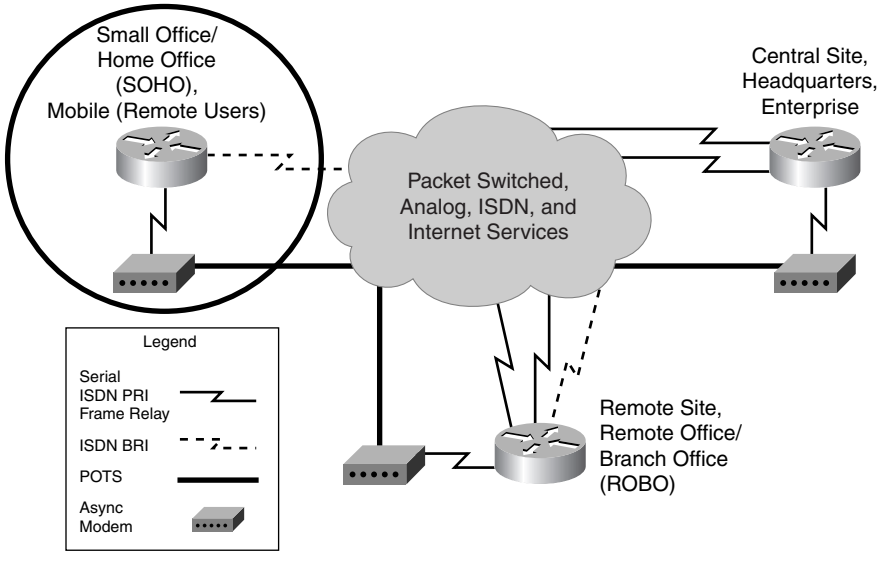
Typical WAN connections employed at SOHO sites are shown in Figure 1-15 and include the following:

- Asynchronous dialup
- ISDN BRI
- Broadband
- Frame Relay (if the user utilizes the link for an extended time, such as half the day)

Typical considerations for a remote site WAN connection follow:

- Cost
- Authentication
- Availability
- SOHO Site Router Equipment

Figure 1-15 *SOHO Site Considerations*



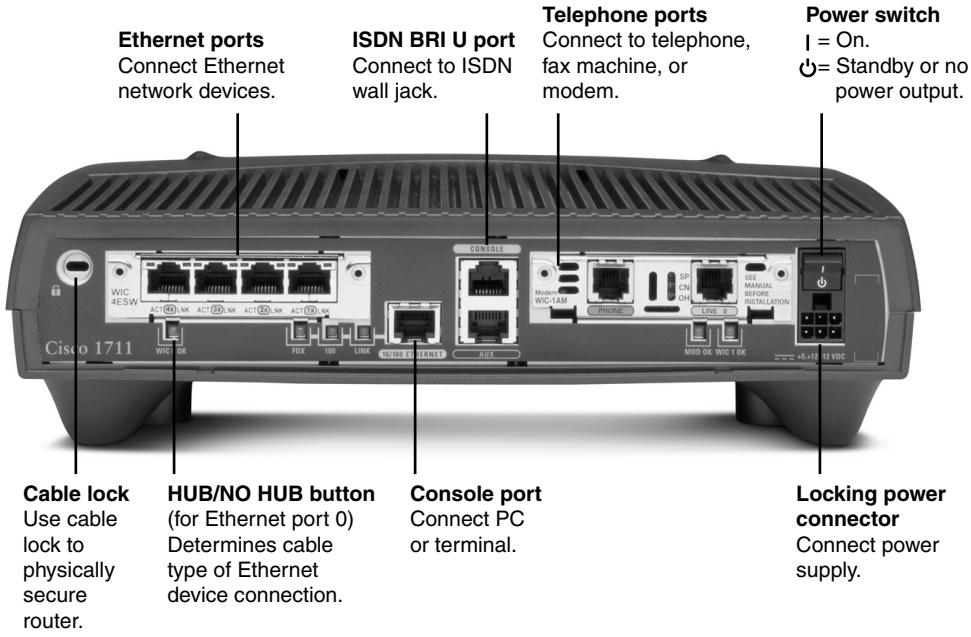
Choose the router that supports the WAN protocols and interfaces you use. As illustrated in Figure 1-15, the 800 series router is an example of a SOHO site router that supports the interfaces required in the network topology.

The following routers are typical Cisco solutions for a SOHO site:

- Cisco 800 series
- Cisco 1700 Series

Figure 1-16 shows SOHO site router equipment.

Figure 1-16 *SOHO Site Router Equipment (Cisco 804 Router)*



Selecting Cisco Remote Access Solutions

Cisco offers access servers, routers, and other equipment that allows connection to the WAN service. The following are highlights of some of the products that are suited for the various company sites:

- The Cisco 800 series routers are the lowest priced Cisco routers, nonmodular or fixed configuration, based on Cisco IOS Software. The 800 series access routers provide big-business networking benefits to small offices and corporate telecommuters. The 800 series offers secure, manageable, high-performance solutions for Internet and corporate LAN access. The 800 series also offers diverse solutions for different types of WAN connections, including ISDN, Serial and ADSL, and Ethernet Broadband.
- The Cisco 1600 series routers are similar to the Cisco 1000 series routers, but also have a slot that accepts a WIC. These cards are shared with the 1700, 2600, and 3600 series and will be shared in future modular branch office type products.
- The Cisco 1700 series access routers deliver optimized security, integration, and flexibility in a desktop form factor for small and medium-sized businesses and small branch offices that want to deploy Internet/intranet access or VPNs. The Cisco 1721 access router features two modular WAN slots that support 1600, 2600, and 3600 data

WAN interface cards, and an autosensing 10/100-Mbps Fast Ethernet LAN port to provide investment protection and flexibility for growth. The 1751 access router provides for Voice over IP (VoIP) technologies.

- The Cisco 2600 series routers feature single or dual fixed LAN interfaces. A network module slot and two WAN interface card slots are available for WAN connections.
- The 3600 and 3700 series multiservice access servers/routers also offer a modular solution for dialup and permanent connectivity over asynchronous, synchronous, and ISDN lines. Up to four network module slots are available for LAN and WAN requirements.
- The Cisco 7200 series routers are also very high-performance, modular, central site routers that support a variety of LAN and WAN technologies. The 7200 series is targeted at large regional offices that require high-density solutions.

Table 1-3 highlights some of the features and WAN options for each series of routers.

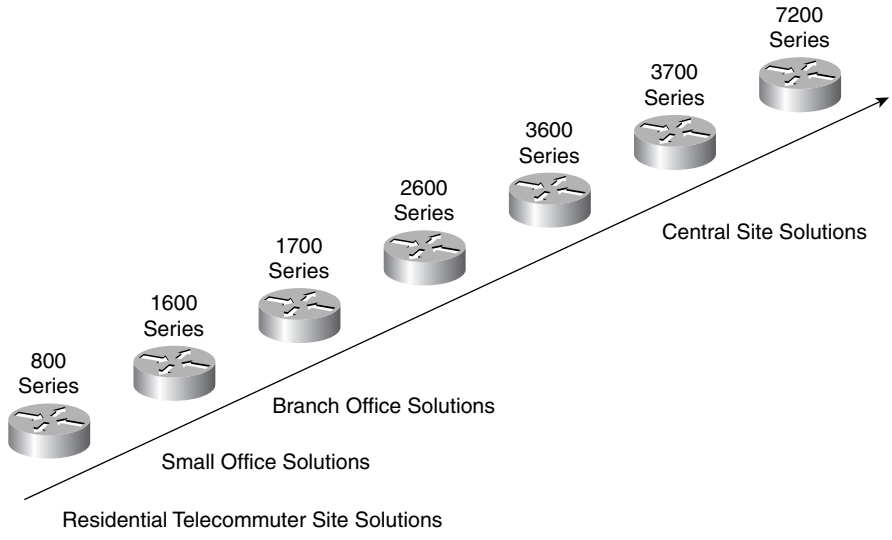
Table 1-3 *WAN Options*

Router	Features
800 series	ISDN BRI, serial connections, basic telephone service ports, Broadband port, entry-level Cisco IOS Software, ADSL, IDSL, and G.SDSL version capabilities.
1600 series	ISDN BRI, 1 WAN interface card slot, Ethernet interface.
1700 series	2 WAN interface card slots; 1751 and 1760 series routers can also support VIC cards. 1710 cannot support WIC or VIC cards but has one 10 Mbps Ethernet connection and one 100 Mbps Fast Ethernet connection
2600 series	Various fixed LAN interface configurations, 1 network module slot, 2 WAN interface card slots.
3600 series	The 3620 has 2 slots, 3640 has 4 slots, and the 3660 has 6 slots.
3700 series	The 3725 has 2 slots, 3745 has 4 slots.
7200 series	Supports a wide range of WAN services with the required high port density necessary for a scalable enterprise WAN.

A power branch is a branch office that offers enhanced capabilities such as those included in the 2600 series routers. Because of its expandability, the 2600 series is common today in branch offices. Refer to Cisco Connection Online (CCO) at www.cisco.com for the most up-to-date information on Cisco equipment.

Figure 1-17 shows Cisco remote access solutions.

Figure 1-17 *Cisco Remote Access Solutions*



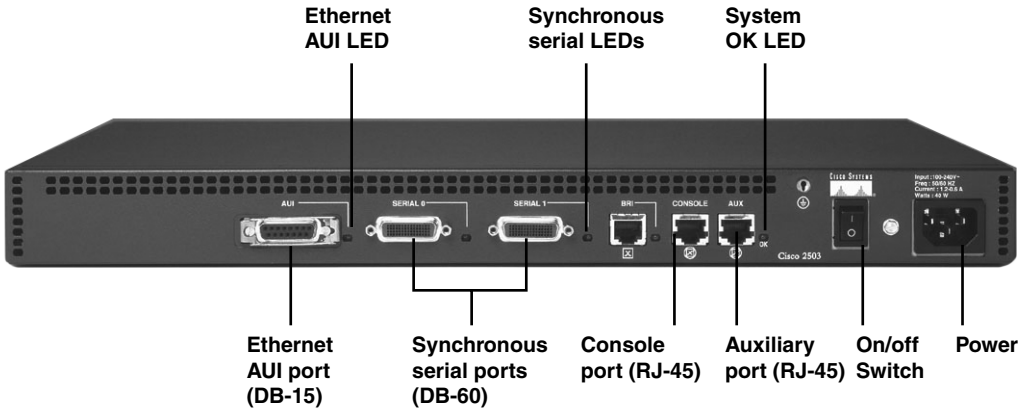
Determining the Appropriate Interfaces: Fixed Interface

The router you select for your WAN connection must offer the interfaces that support your WAN connection. An interface on a router that cannot be removed or replaced is referred to as a *fixed interface*. Typical interfaces found on a Cisco router and the typical WAN connections support the following:

- **Asynchronous serial**—Used with a modem, supports asynchronous dialup connections
- **Synchronous serial**—Supports connections such as leased lines and Frame Relay.
- **Ethernet**—Supports Broadband connections
- **BRI**—Supports ISDN BRI connections
- **T1 or E1**—Supports connections such as leased lines, dialup, ISDN PRI, and Frame Relay

Fixed-configuration routers are available with predetermined fixed LAN and WAN interface options. Fixed-configuration routers cannot use WIC or network modules because they are fixed configuration routers. However, once purchased, the interfaces available are limited only to those that are factory installed. Figure 1-18 shows a fixed interface.

Figure 1-18 *Fixed Interface*

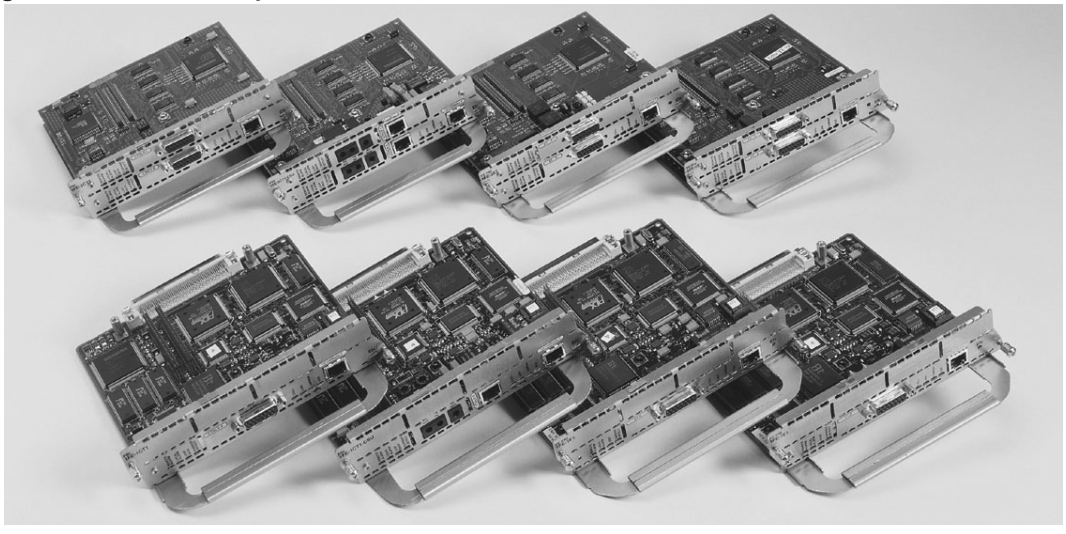


Determining the Appropriate Interfaces: Modular Interface

If you select a fixed-configuration router, you receive the router with the interfaces already built in. However, you cannot add or change interfaces on a fixed-configuration router.

Modular routers and access servers are built with one or more slots that allow you to customize the box. You can determine the types of interfaces on the router by selecting various feature cards, network modules, or WAN interface cards that install into the box. Although modular routers require additional equipment to the physical router, they are more scalable as your network grows and your needs change. Figure 1-19 shows an example of a modular interface.

Figure 1-19 *Modular Interface*



Assembling and Cabling the Network

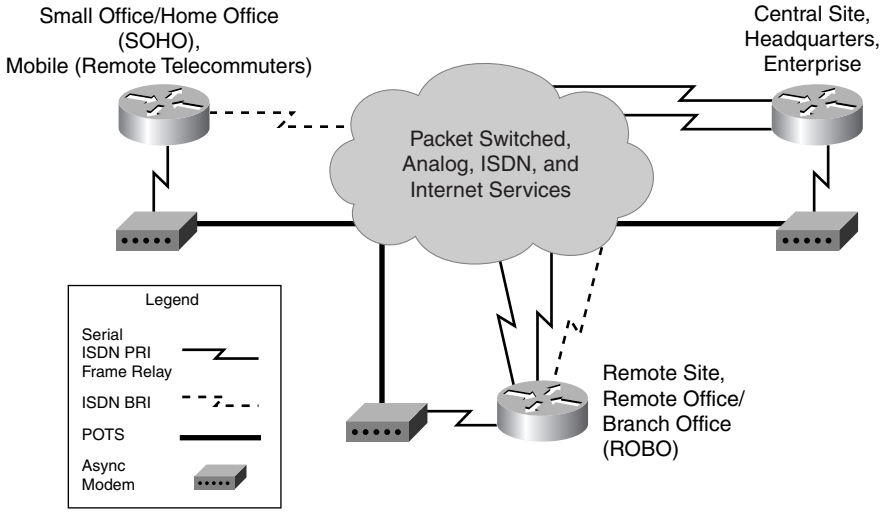
Figure 1-20 illustrates the cable connections available for the various WAN types. The following text lists some of the cable connection types:

- **Asynchronous connections**—Asynchronous connections require RJ-11 cables attached from the modem line port to the telephone company jack. If you are using an external modem attached to a Cisco router, you must also use an EIA/TIA-232 cable to attach the modem to the router's serial interface. The DB-60 end of the cable connects to the router. The DB-25 end attaches to the modem.
- **ISDN BRI**—ISDN BRI connection interfaces require RJ-45 cables to connect the BRI interface to the ISDN network. The BRI modules and BRI WAN interface cards are available with either an S/T interface that requires an external NT1, or a U interface with a built-in NT1.
- **ISDN PRI (North America)**—Channelized T1 (CT1)/PRI modules are available with or without a built-in CSU. If you use an external CSU, attach a female DB-15 cable to the router's interface. The other end of the straight-through cable attach to the CSU, which in turn attaches to the ISDN network. Routers with internal CSU modules attach directly to the ISDN network with a standard RJ-48 connector.
- **ISDN PRI (Europe)**—Channelized E1 (CE1)/PRI modules are available with balanced and unbalanced interfaces. CE1/PRI-balanced modules provide a 120-ohm E1 interface for network connections. The unbalanced modules provide a 75-ohm E1 interface for network connections. Four serial cables are available from Cisco for the CE1/PRI module. All four cables have DB-15 connectors on the router end and BNC, DB-15, twinax, or RJ-45 connectors on the network end.
- **Frame Relay**—If you establish a Frame Relay serial connection, Cisco routers support the following signaling standards: EIA/TIA-232, EIA/TIA-449, V.35, X.21, and EIA/TIA-530. Cisco supplies a DB-60 shielded serial transition cable with the appropriate connector for the standard you specify. The router end of the shielded serial transition cable has a DB-60 connector, which connects to the DB-60 port on the router's serial interface. The other end of the serial transition cable depends on the standard you specify.
- **Broadband**—Connections generally require an Ethernet interface port and service provider equipment. Data service is generally provided through equipment from the provider and converted to RJ-45 by the customer.

NOTE The RJ-48 and DB-15 cables can also be used for Frame Relay connections. They can be plugged into a T1 carrier interface. After a channel group is configured, Frame Relay encapsulation can be run over the connection.

NOTE For specific cabling information, refer to the installation and configuration guide that came with your router. For information regarding cable pinouts, refer to the *Cable Specifications* documentation. It is available on the Cisco website and in the installation and configuration guide that came with your router.

Figure 1-20 *Assembling and Cabling the Network*

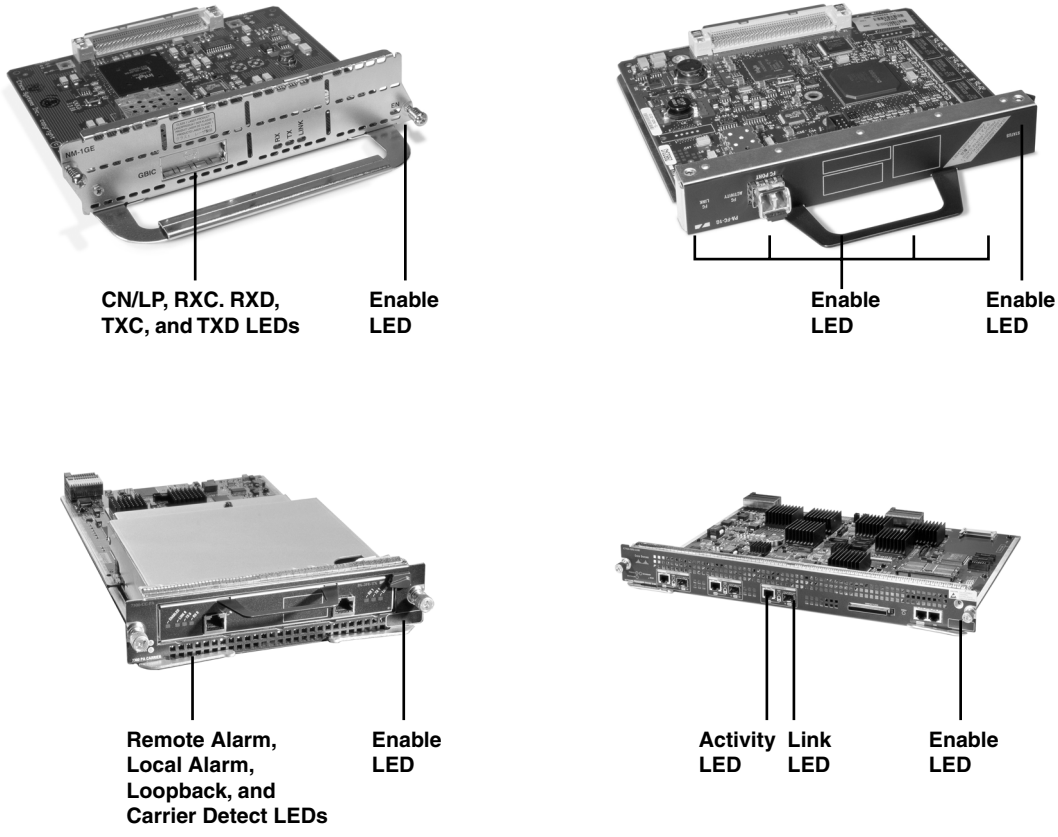


Verifying Network Installation

Each central site router has light emitting diodes (LED) displays that allow you to verify that the router components are installed and functioning properly. An example is shown in Figure 1-21.

NOTE For LED information specific to your router, refer to the installation and configuration guide that accompanied your router.

Figure 1-21 *Verifying Central Site Installation*



On the Cisco 3600 router, the LEDs on the front of the router enable you to determine router performance and operation. The ready LED indicates a functional module has been installed in the indicated slot. If the READY LED is off, the slot is empty or the module is not functional. The active LED blinks to indicate network activity on the module installed in the indicated slot.

All network modules have an ENABLE (EN) LED. The ENABLE LED indicates that the module has passed its self-tests and is available to the router. If the ENABLE LED is not on, this might indicate a network module not being properly seated, the router might not have the proper IOS version, or the module might be bad.

Each Ethernet port has two LEDs. The activity (ACT) LED indicates that the router is sending or receiving Ethernet transmissions. The LINK LED indicates that the Ethernet port is receiving the link-integrity signal from the hub or switch. The LINK LED is only used for the 10BASE-T connection and not for the AUI connection on the network module.

Each PRI network module has four LEDs in addition to the enable LED. These LEDs are as follows:

- **REMOTE ALARM**—Designates a remote alarm condition
- **LOCAL ALARM**—Designates a local alarm condition
- **LOOPBACK**—Designates a loopback condition
- **CARRIER DETECT**—Specifies that you received the carrier on the telephone company link

Digital modem modules have five LEDs in addition to the enable LED, one for each Modem ISDN Channel Aggregation (MICA) technology module bank. The LEDs blink during initialization. After the enable LED comes on, the MICA module LEDs indicate that the corresponding MICA module is functioning. If a MICA module fails its diagnostics, or if no MICA module is installed in a position, its LED remains off.

Each port on the serial network module has the additional LEDs. These LEDs are as follows:

- **CN/LP**—Connect when green, loopback when yellow
- **RXC**—Receive clock
- **RXD**—Receive activity
- **TXC**—Transmit clock
- **TXD**:—Transmit activity

Verifying Branch Office Installation

Each branch office and telecommuter router has LED displays that allow you to verify that the router components are installed and functioning properly.

For LED information specific to your router, refer to the installation and configuration guide that accompanied your router. An example is shown in Figure 1-22.

On the 1721 routers, you can use the LEDs on the front of the router to determine router performance and operation. The LEDs are as follows:

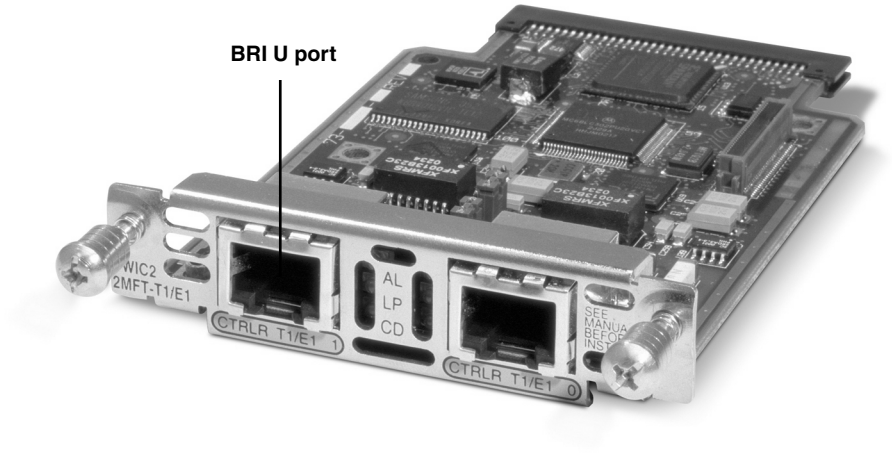
- **SYSTEM PWR**—The green system power LED indicates the router is turned on and DC power is being supplied.
- **SYSTEM OK**—The green system OK LED indicates the router has successfully booted. This LED blinks while in the boot cycle.
- **ETH ACT**—The green LAN activity LED indicates data is being sent to or received from the local Ethernet LAN.
- **ETH COL**—A flashing yellow LAN collision LED indicates frame collisions on the local Ethernet LAN.

- **WIC0 ACT/CH0**—The green WAN interface card connection LED indicates an active connection on the WAN interface card port.
- **WIC0 ACT/CH1**—The green WAN interface card connection LED indicates an active connection on the WAN interface card port.
- **WIC1 ACT/CH0**—The green WAN interface card connection LED indicates an active connection on the WAN interface card port.
- **WIC1 ACT/CH1**—The green WAN interface card activity LED indicates an active connection on the WAN interface card port.

The serial WAN interface card has several LEDs that indicate data is being sent over the WAN interface card serial ports.

The ISDN BRI U interface card has several LEDs that indicate data is being sent over the WAN ISDN port.

Figure 1-22 *Verifying Branch Office Site Installation*



WIC 2A/S

Verifying Small Office Home Office Installation

Each small office home office router has LED displays that allow you to verify that the router components are installed and functioning properly.

On the 800 series routers, you can use the LEDs on the back of the router to determine router performance and operation. The LEDs are shown in Table 1-4.

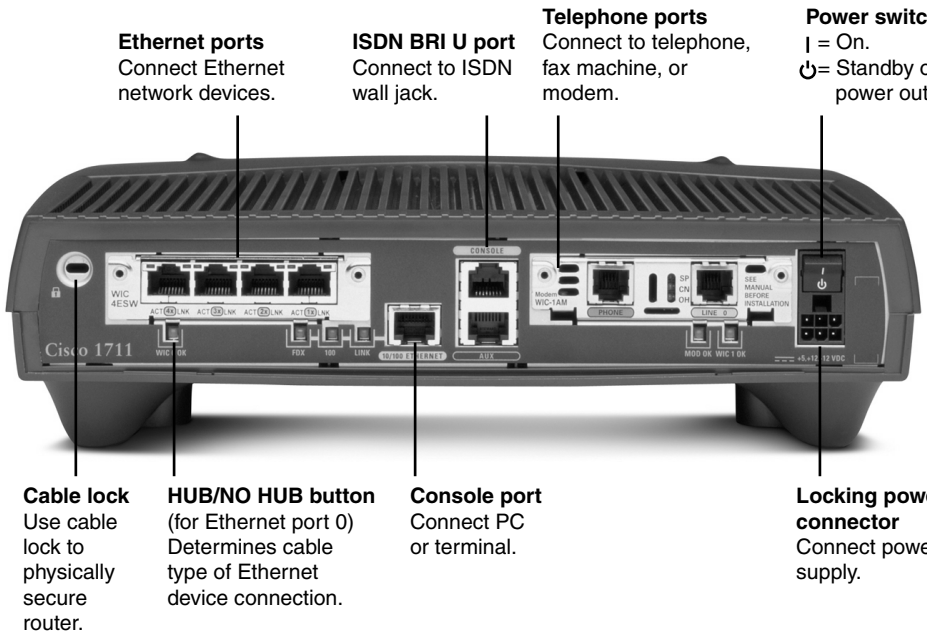
Table 1-4 *800 Series Router LEDs*

LED	Color	Function
OK	Green	On when power is supplied to the router and when the router completes the self-test procedure and begins operating.
NT1	Green	Not applicable for Cisco 801 and 803 routers. On when the internal NT1 and the ISDN switch are synchronized. Blinks when the internal NT1 and the ISDN switch are attempting to synchronize.
LINE	Green	On when the ISDN interface and the ISDN terminal device are synchronized.
LAN	Green	On when packets are sent to or received from an Ethernet port.
LAN RXD	Green	Blinks when an Ethernet port receives a packet.
LAN TXD	Green	Blinks when an Ethernet port sends a packet.
LKØ, LK1, LK2, LK3	Green	Cisco 803 and 804 routers only. On when the Ethernet device is connected. Off when the Ethernet device is not connected. Blinks when the connection has a problem.
ETHERNET 1, 2, 3, 4	Green	Cisco 804 IDSL routers only. On when the Ethernet device is connected. Off when the Ethernet device is not connected. Blinks when the connection has a problem.
CH1	Orange	Blinks when placing or receiving a call on the first ISDN B channel. On when a call is connected on the first ISDN B channel.
CH1 RXD	Orange	Blinks when packets are received from the first ISDN B channel.
CH1 TXD	Orange	Blinks when packets are sent from the first ISDN B channel.
CH2	Orange	Blinks when placing or receiving a call on the second ISDN B channel. On when a call is connected on the second ISDN B channel. For IDSL routers.
CH2 RXD	Orange	Blinks when packets are received from the second ISDN B channel.
CH2 TXD	Orange	Blinks when packets are sent from the second ISDN B channel.
PH1,PH2	Green	Cisco 803 and 804 routers only. On when basic telephone service is in use.
LINK	Green	On the back panel of the Cisco 801, 802, and 802 IDSL routers only. On when Ethernet device is connected. Blinks when the connection has a problem.

NOTE On Cisco 802 IDSL and Cisco 804 IDSL routers, either CH1 or CH2 is on if the router has an active data connection and the line speed is 64 kbps. CH1 and CH2 are both on if the router has an active data connection and the line speed is 128 or 144 kbps

For LED information specific to your router, refer to the installation and configuration guide that accompanied your router. An example is shown in Figure 1-23.

Figure 1-23 *Verifying SOHO Site Installation*



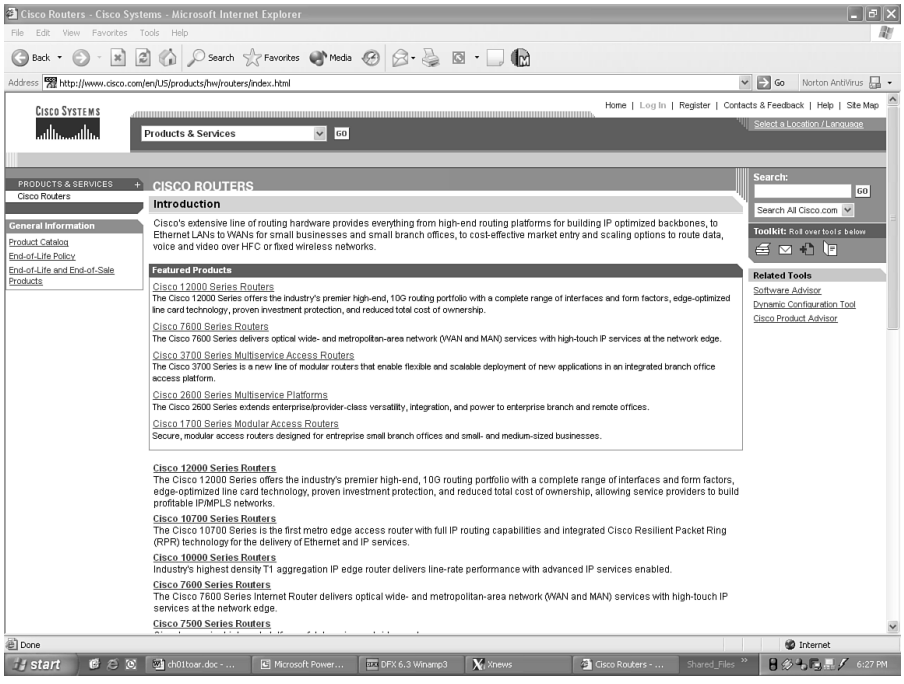
Selecting Products with Cisco Product Selection Tools

To assist you with product selection, Cisco has extensive documentation and product specifications on its website at www.cisco.com/en/US/products/hw/routers/index.html. Also refer to the Cisco Products Quick Reference Guide that is also available to the reader online at http://www.cisco.com/warp/public/752/qrg/.

Figure 1-24 shows the Cisco Product Selection Tool. You can also find product selection and configuration tools. These tools are designed to help you determine and configure the router that best suits your requirements.

NOTE Because technology and product offerings change frequently, access this website for the most up-to-date product information. This course does not offer instruction about LAN switches and hubs.

Figure 1-24 *Selecting Products with Cisco Product Selection Tools*



Summary

In this chapter, you learned about WAN connections and how to determine the requirements of a central site, a branch office, and a remote site. You also learned how to select Cisco products to suit the specific needs of each site and how to utilize Cisco website resources to view and select the proper equipment. In addition, you learned how to identify and connect the necessary components for central site, branch office, and small office WAN solutions.

Chapter Review Questions

The following questions provide you with an opportunity to test your knowledge of the topics covered in this chapter. You can find the answers to these questions in Appendix A, "Answers to Chapter Review Questions."

1. Which major WAN connection characteristic includes consideration of the elapsed time of the connection?
   - a. Data rate
   - b. Termination
   - c. Transmission media
   - d. Connection duration
2. Dedicated lines are also known as what?
   - a. Synchronous lines
   - b. Asynchronous lines
   - c. Leased lines
   - d. Dedicated lines
3. Dedicated permanent connections are most often made using which type of router interface ports?
   - a. Ethernet ports
   - b. Synchronous serial ports
   - c. Console ports
   - d. ISDN BRI B channels
4. Which of the following conditions is appropriate for asynchronous serial connections?
   - a. Your network would use it as its primary WAN connection for sending huge amounts of data traffic.
   - b. Your network needs a very reliable high-speed connection.
   - c. Your network is a small remote site and does not require a high-speed WAN connection.
   - d. Your network has five users, and they send large files to a central site that is located more than 35 miles away.

5 Which of the following is considered an on-demand connection?

a 100-Mbps LAN connection

b Broadband connection

c T1 synchronous serial connection

d ISDN BRI connection

6 What physical connection is used for high-speed ISDN access in North America?

a A 23B + 1D Channelized T1 line

b A 2B + 1D Channelized BRI

c A 30B + 1D Channelized E1 line

d An ISDN Network Terminal Adapter

7 Packet switching is a networking technology based on the transmission of data in what form?

a Indices

b Time slices

c Bit streams

d Small units

8 What is the most common problem a remote user typically encounters in obtaining broadband access service?

a Lack of area coverage by broadband providers

b Large initial connection fee charged by broadband providers

c High cost of connections as compared to other dedicated WAN services

d Reduced bandwidth as compared to on-demand WAN services

9 What is the fixed length of an Asynchronous Transfer Mode (ATM) cell?

a 128-byte cells

b 56-byte cells

c 53-byte cells

d 64-byte cells

10 What component does PPP use to negotiate and set up control options on the WAN data link?

- **a** Network Control Protocol (NCP)
- **b** Link Control Protocol (LCP)
- **c** File Transfer Protocol (FTP)
- **d** Trivial File Transfer Protocol (TFTP)

11 In Frame Relay, what is the DLCI?

- **a** Data-link control identifier
- **b** Data-level control identifier
- **c** Data-link connection identifier
- **d** Data-level connection identifier

12 What percentage of the information services budget do WAN costs typically take?

- **a** 10 percent
- **b** 25 percent
- **c** 50 percent
- **d** 80 percent

13 Which of the following is an advantage of using an asynchronous dialup connection?

- **a** Its high-speed connection.
- **b** The ability to connect to the WAN from any active phone line.
- **c** It is an always-on connection.
- **d** You can use the phone connection for voice calls at the same time.

14 Which of the following technologies would small office, home office, and branch office users use to gain access to a very secure central site?

- **a** Virtual private network (VPN) technologies
- **b** Standard password authentication protection technologies
- **c** Unsecured high-speed broadband connection technologies
- **d** Slower-speed asynchronous dialup technologies

15 Which of the following is most typically used to permit traffic onto a network or deny that traffic?

- **a** Access control lists
- **b** Password authentication
- **c** Accounting software
- **d** Record management software

16 Which of the following Cisco series routers can offer the highest port density?

- **a** Cisco 1700 series
- **b** Cisco 7200 series
- **c** Cisco 2600 series
- **d** Cisco 800 series

17 Which of the following router interface supports the Frame Relay connection?

- **a** Synchronous serial
- **b** Ethernet
- **c** BRI
- **d** Asynchronous serial