Connecting to the WAN

Objectives

Upon completion of this chapter

- What is the purpose of a WAN?

- How does a circuit-switched network differ from a packet-switched network?

- How do service provider networks connect to enterprise networks?

- How do the link connection options available from private WAN infrastructures and public WAN infrastructures differ?

- What questions should you answer when choosing a WAN link connection?

Key Terms

This chapter uses the following key terms. You can find the definitions in the glossary.

Introduction (2.0.1.1)

Businesses must connect local-area networks (LANs) together to provide communications between them, even when these LANs are far apart. Wide-area networks (WANs) are used to connect remote LANs together. A WAN may cover a city, country, or global region. A WAN is owned by a service provider, and a business pays a fee to use the provider's WAN network services.

Different technologies are used for WANs than for LANs. This chapter introduces WAN standards, technologies, and purposes. It covers selecting the appropriate WAN technologies, services, and devices to meet the changing business requirements of an evolving enterprise.

Class Activity 2.0.1.2: Branching Out

Your medium-size company is opening a new branch office to serve a wider, client-based network. This branch will focus on regular day-to-day network operations, but will also provide TelePresence, web conferencing, IP telephony, video on demand, and wireless services.

Although you know that an ISP can provide WAN routers and switches to accommodate the branch office connectivity for the network, you prefer to use your own customer premises equipment (CPE). To ensure interoperability, Cisco devices have been used in all other branch-office WANs.

As the branch-office network administrator, it is your responsibility to research possible network devices for purchase and use over the WAN.

WAN Technologies Overview (2.1)

As an organization expands, WAN connections are necessary. This section discusses the purpose of WANs, introduces WAN terminology, WAN devices, and circuit-switch / packet-switch networks.

Why a WAN? (2.1.1.1)

A WAN operates beyond the geographic scope of a LAN. As shown in Figure 2-1, WANs are used to interconnect the enterprise LAN to remote LANs in branch sites and telecommuter sites.
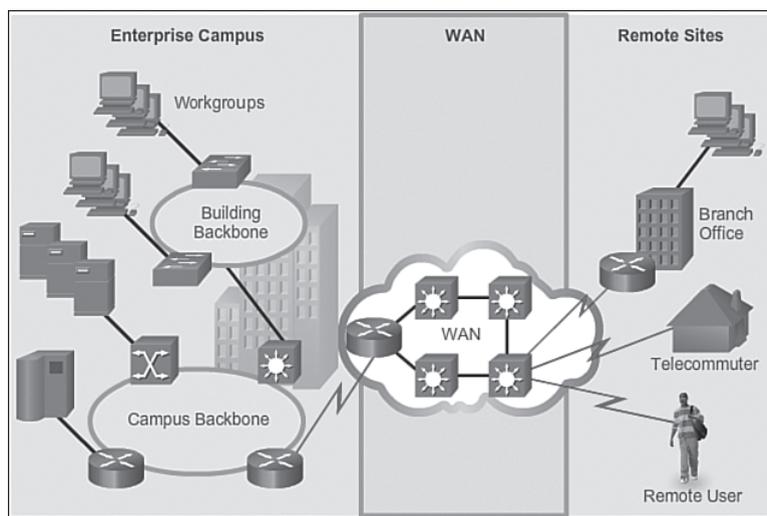
Figure 2-1   WANs Interconnect Users and LANs

A WAN is owned by a *service provider*. An organization must pay a fee to use the provider's network services to connect remote sites. WAN service providers include carriers, such as a telephone network, cable company, or satellite service. Service providers provide links to interconnect remote sites for the purpose of transporting data, voice, and video.

In contrast, LANs are typically owned by the organization and used to connect local computers, peripherals, and other devices within a single building or other small geographic area.

Are WANs Necessary? (2.1.1.2)

Without WANs, LANs would be a series of isolated networks. LANs provide both speed and cost-efficiency for transmitting data over relatively small geographic areas. However, as organizations expand, businesses require communication among geographically separated sites. The following are some examples:

- Regional or branch offices of an organization need to be able to communicate and share data with the central site.

- Organizations need to share information with other customer organizations. For example, software manufacturers routinely communicate product and promotional information to distributors that sell their products to end users.

- Employees who travel on company business frequently need to access information that resides on their corporate networks.

Home computer users also need to send and receive data across increasingly larger distances. Here are some examples:

- Consumers now commonly communicate over the Internet with banks, stores, and a variety of providers of goods and services.

- Students do research for classes by accessing library indexes and publications located in other parts of their country and in other parts of the world.

It is not feasible to connect computers across a country, or around the world, with physical cables. Therefore, different technologies have evolved to support this communication requirement. Increasingly, the Internet is being used as an inexpensive alternative to enterprise WANs. New technologies are available to businesses to provide security and privacy for their Internet communications and transactions. WANs used by themselves, or in concert with the Internet, allow organizations and individuals to meet their wide-area communication needs.

Evolving Networks (2.1.1.3)

Every business is unique, and how an organization grows depends on many factors. These factors include the type of products or service the business sells, the management philosophy of the owners, and the economic climate of the country in which the business operates.

In slow economic times, many businesses focus on increasing their profitability by improving the efficiency of their existing operations, increasing employee productivity, and lowering operating costs. Establishing and managing networks can represent significant installation and operating expenses. To justify such a large expense, companies expect their networks to perform optimally and to be able to deliver an ever increasing array of services and applications to support productivity and profitability.

The example used in this chapter is of a fictitious company called SPAN Engineering. The following topics provide an example of how the network requirements of SPAN Engineering change as the company grows from a small local business into a global enterprise.

Small Office (2.1.1.4)

SPAN Engineering is an environmental consulting firm that has developed a special process for converting household waste into electricity. SPAN Engineering is developing a small pilot project for a municipal government in its local area. The company, which has been in business for 4 years, has grown to include 15 employees: 6 engineers, 4 computer-aided drawing (CAD) designers, a receptionist, 2 senior partners, and 2 office assistants.

SPAN Engineering's management is working to win full-scale contracts after the pilot project successfully demonstrates the feasibility of their process. Until then, the company must manage its costs carefully.

For their small office, SPAN Engineering uses a single LAN to share information between computers, and to share peripherals, such as a printer, a large-scale plotter (to print engineering drawings), and fax equipment. They have recently upgraded their LAN to provide inexpensive Voice over IP (VoIP) service to save on the costs of separate phone lines for their employees.

The SPAN Engineering network consists of a small office as shown in Figure 2-2.
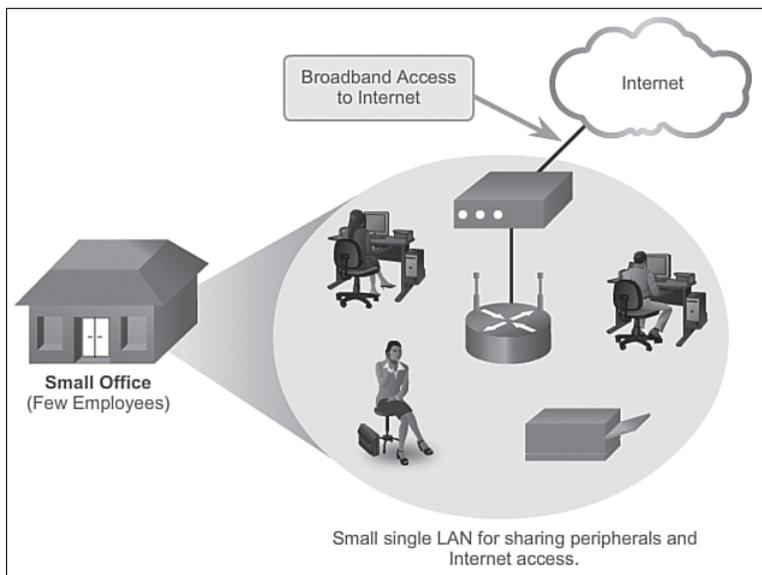
Figure 2-2   Connecting a Small Office

Connection to the Internet is through a common broadband service called *digital subscriber line (DSL)*, which is supplied by their local telephone service provider. With so few employees, bandwidth is not a significant problem.

The company cannot afford in-house IT support staff, and uses support services purchased from the DSL provider. The company also uses a hosting service rather than purchasing and operating its own FTP and email servers.

Campus Network (2.1.1.5)

Five years later, SPAN Engineering has grown rapidly. The company was contracted to design and implement a full-size waste-conversion facility soon after the successful implementation of their first pilot plant. Since then, SPAN has won other projects in neighboring municipalities, and in other parts of the country.

To handle the additional workload, the business has hired more staff and leased more office space. It is now a small- to medium-size business with several hundred employees. Many projects are being developed at the same time, and each requires a project manager and support staff. The company has organized itself into functional departments, with each department having its own organizational team. To meet its growing needs, the company has moved into several floors of a larger office building, as shown in Figure 2-3.
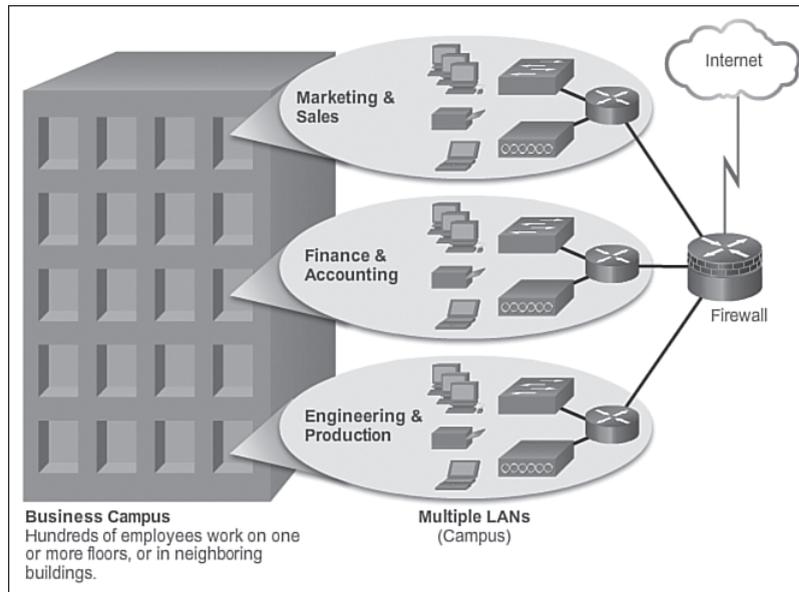
Figure 2-3   Connecting a Campus Network

As the business has expanded, the network has also grown. Instead of a single small LAN, the network now consists of several subnetworks, each devoted to a different department. For example, all the engineering staff is on one LAN, while the marketing staff is on another LAN.

These multiple LANs are joined to create a company-wide campus network which spans several floors of the building.

The business now has in-house IT staff to support and maintain the network. The network includes dedicated servers for email, data transfer, and file storage, and web-based productivity tools and applications. There is also a company intranet to provide in-house documents and information to employees. An extranet provides project information to designated customers.

Branch Networks (2.1.1.6)

Another 6 years later, SPAN Engineering has been so successful with its patented process that demand for its services has skyrocketed. New projects are underway in multiple cities. To manage those projects, the company has opened small branch offices closer to the project sites.

This situation presents new challenges to the IT team. To manage the delivery of information and services throughout the company, SPAN Engineering now has a data center, which houses the various databases and servers of the company. To ensure that all parts of the business are able to access the same services and applications regardless of where the offices are located, the company must now implement a WAN, as shown in Figure 2-4.
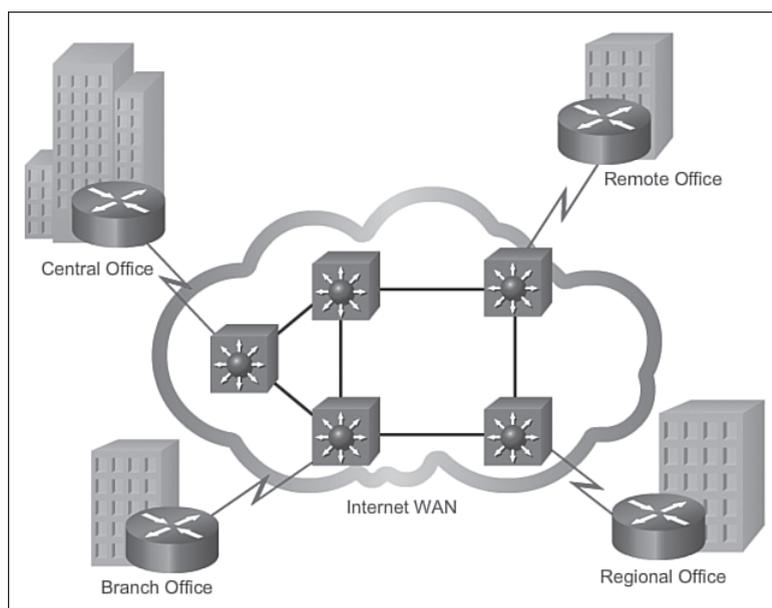
Figure 2-4   Connecting Branch Networks

Connecting to its branch sites may occur over dedicated private lines or by using the Internet. For its branch office that is in a nearby city, the company decides to use private dedicated lines through their local service provider. However, for its regional office and remote office located in another country, the Internet is an attractive WAN connection option. Although connecting offices through the Internet is economical, it introduces security and privacy issues that the IT team must address.

Distributed Network (2.1.1.7)

SPAN Engineering has now been in business for 20 years and has grown to thousands of employees distributed in offices worldwide. The cost of the network and its related services is a significant expense. The company is looking to provide its employees with the best network services at the lowest cost. Optimized network services would allow each employee to work at a high rate of efficiency.

To increase profitability, SPAN Engineering must reduce its operating expenses. It has relocated some of its office facilities to less-expensive areas. The company is also encouraging teleworking and virtual teams. Web-based applications, including web conferencing, e-learning, and online collaboration tools, are being used to increase productivity and reduce costs. Site-to-site and remote access virtual private networks (VPNs) enable the company to use the Internet to connect easily and securely with employees and facilities around the world. To meet these requirements, the network must provide the necessary converged services and secure Internet WAN connectivity to remote offices and individuals, as shown in Figure 2-5.
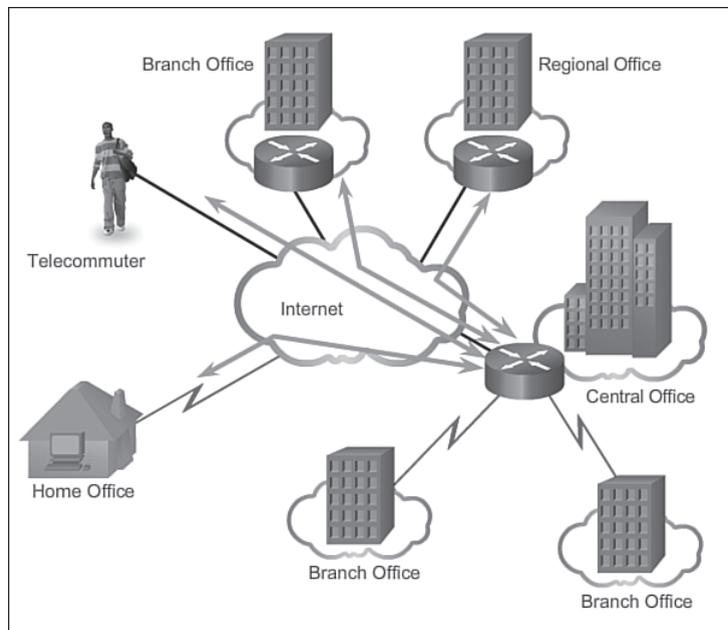
Figure 2-5   Connecting a Global Enterprise Network

As seen in this example, network requirements of a company can change dramatically as the company grows over time. Distributing employees saves costs in many ways, but it puts increased demands on the network. Not only must a network meet the day-to-day operational needs of the business, but it must also be able to adapt and grow as the company changes. Network designers and administrators meet

these challenges by carefully choosing network technologies, protocols, and service providers, and by optimizing their networks using many of the network design techniques and architectures described in this course.

Activity 2.1.1.8: Identify WAN Topologies

Go to the course online to perform this practice activity.

WAN Operations (2.1.2)

This topic introduces common WAN terminology and devices and differentiates between circuit-switch and packet-switch networks.

WANs in the OSI Model (2.1.2.1)

As shown in Figure 2-6, WAN operations focus primarily on the physical layer (OSI Layer 1) and the data link layer (OSI Layer 2).
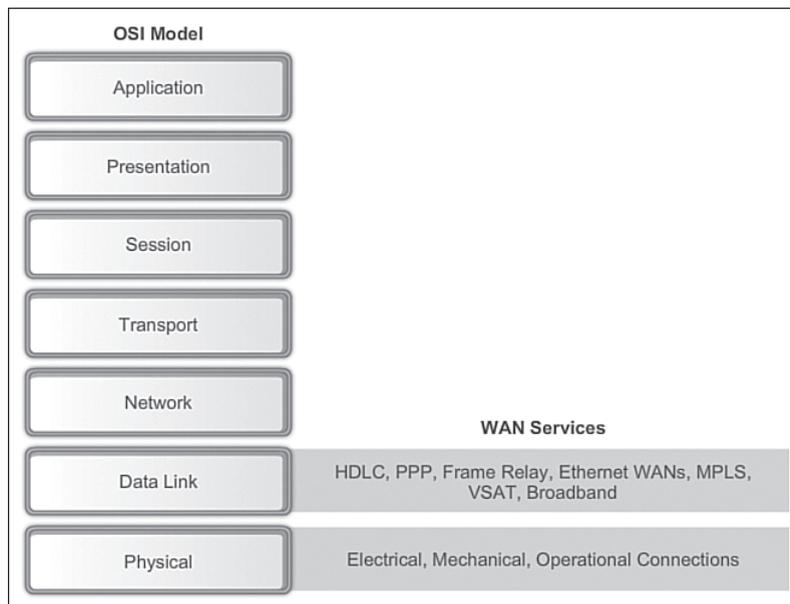
Figure 2-6   WANs Operate in Layer 1 and Layer 2

WAN access standards typically describe both physical layer delivery methods and data link layer requirements, including physical addressing, flow control, and encapsulation.

WAN access standards are defined and managed by a number of recognized authorities, including the

- Telecommunication Industry Association and the Electronic Industries Alliance (TIA/EIA)

- International Organization for Standardization (ISO)

- Institute of Electrical and Electronics Engineers (IEEE)

Layer 1 protocols describe how to provide electrical, mechanical, operational, and functional connections to the services of a communications service provider.

Layer 2 protocols define how data is encapsulated for transmission toward a remote location, and the mechanisms for transferring the resulting frames. A variety of different technologies are used, such as the *Point-to-Point Protocol (PPP)*, *Frame Relay*, and *Asynchronous Transfer Mode (ATM)*. Some of these protocols use the same basic framing or a subset of the *High-Level Data Link Control (HDLC)* mechanism.

Most WAN links are point to point. For this reason, the address field in the Layer 2 frame is usually not used.

Common WAN Terminology (2.1.2.2)

One primary difference between a WAN and a LAN is that an organization must subscribe to an outside WAN service provider and use the WAN carrier network services to interconnect its sites and users. A WAN uses data links provided by carrier services to access the Internet and connect different locations of an organization to each other, to locations of other organizations, to external services, and to remote users.

The physical layer of a WAN describes the physical connections between the company network and the service provider network. As illustrated in Figure 2-7, common terminology is used to describe WAN components and reference points.
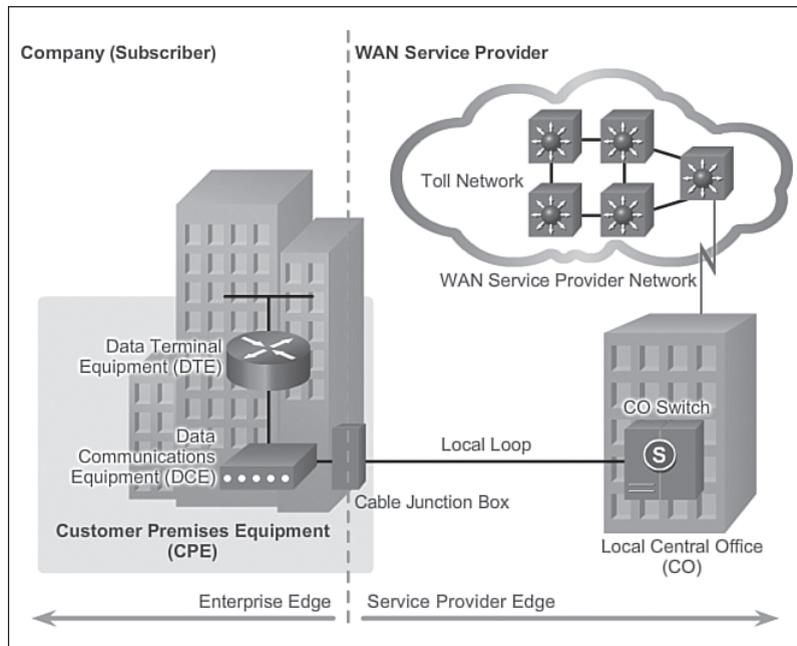
Figure 2-7   Common WAN Terminology

Specifically, these terms include

- *Customer premises equipment (CPE)*: The devices and inside wiring located on the enterprise edge connecting to a carrier link. The subscriber either owns the CPE or leases the CPE from the service provider. A subscriber, in this context, is a company that arranges for WAN services from a service provider.

- *Data communications equipment (DCE)*: Also called data circuit-terminating equipment, the DCE consists of devices that put data on the local loop. The DCE primarily provides an interface to connect subscribers to a communication link on the WAN cloud.

- *Data terminal equipment (DTE)*: The customer devices that pass the data from a customer network or host computer for transmission over the WAN. The DTE connects to the local loop through the DCE.

- *Demarcation point*: A point established in a building or complex to separate customer equipment from service provider equipment. Physically, the demarcation point is the cabling junction box, located on the customer premises, that connects the CPE wiring to the local loop. It is usually placed for easy access by a technician. The demarcation point is the place where the responsibility for the connection changes from the user to the service provider. When problems arise, it is necessary to determine whether the user or the service provider is responsible for troubleshooting or repair.

- *Local loop*: The actual copper or fiber cable that connects the CPE to the CO of the service provider. The local loop is also sometimes called the "last mile."

- *Central office (CO)*: The CO is the local service provider facility or building that connects the CPE to the provider network.

- *Toll network*: This consists of the long-haul, all-digital, fiber-optic communications lines, switches, routers, and other equipment inside the WAN provider network.

WAN Devices (2.1.2.3)

As illustrated in Figure 2-8, there are various methods, and therefore devices, that are used to access the WAN connection. Service providers also have specific WAN devices within their network and devices that are required to interconnect to other WAN providers.
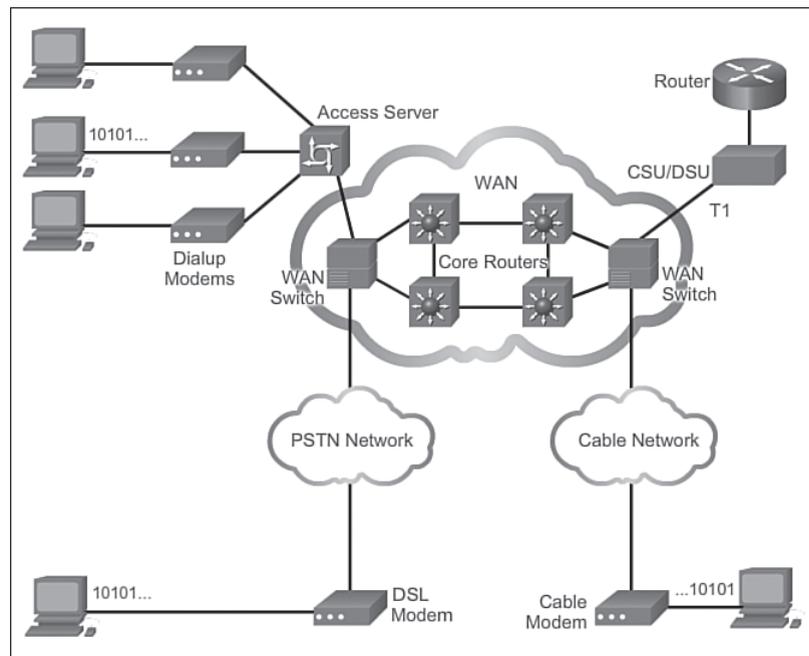
Figure 2-8 WAN Devices

The example in the figure identifies the following WAN devices:

- *Dialup modem*: Considered to be a legacy WAN technology, a voiceband modem converts (i.e., modulates) the digital signals produced by a computer into voice frequencies that can be transmitted over the analog lines of the public telephone network. On the other side of the connection, another modem converts the sounds back into a digital signal (i.e., demodulates) for input to a computer or network connection.

- *Access server*: Devices used to concentrate the dial-in and dial-out user communications of dialup modems. Considered to be a legacy technology, an access server may have a mixture of analog and digital interfaces and support hundreds of simultaneous users.

- *Broadband modem*: A type of digital modem used with high-speed DSL or cable Internet service. Both operate in a similar manner to the voiceband modem, but use higher broadband frequencies and transmission speeds.

- *Channel service unit / data service unit (CSU/DSU)*: Digital leased lines require a CSU and a DSU. A CSU/DSU can be a separate device like a modem or it can be an interface on a router. The CSU provides termination for the digital signal and ensures connection integrity through error correction and line monitoring. The DSU converts the line frames into frames that the LAN can interpret and vice versa.

- **WAN switch**: A multiport internetworking device used in service provider networks. These devices typically switch traffic, such as Frame Relay or ATM and operate at Layer 2.

- **Router**: This is a CPE device that provides internetworking and WAN access interface ports used to connect to the service provider network. These interfaces may be serial connections, Ethernet, or other WAN interfaces. With some types of WAN interfaces, an external device, such as a DSU/CSU or modem (analog, cable, or DSL), is required to connect the router to the local service provider.

- **Core router/multilayer switch**: These are the routers and multilayer switches that reside within the service provider WAN backbone. To fulfill this role, the devices must be able to support routing protocols being used in the core and multiple high speed interfaces used in the WAN core backbone. They must also be able to forward IP packets at full speed on all of those interfaces. Key core routers interconnect to other provider core routers.

Note

The preceding list is not exhaustive, and other devices may be required depending on the WAN access technology chosen.

The type of devices used depends on the WAN technology implemented. These WAN technologies are implemented over either circuit-switched or packet-switched networks.

Circuit-Switched Networks (2.1.2.4)

A *circuit-switched network* is one that establishes a dedicated circuit (or channel) between nodes and terminals before the users may communicate. As illustrated in

Figure 2-9, circuit switching dynamically establishes a dedicated virtual connection for voice or data between a sender and a receiver. Before communication can start, it is necessary to establish the connection through the network of the service provider. It is important to note that the circuit must remain established and never change or communication will be terminated.
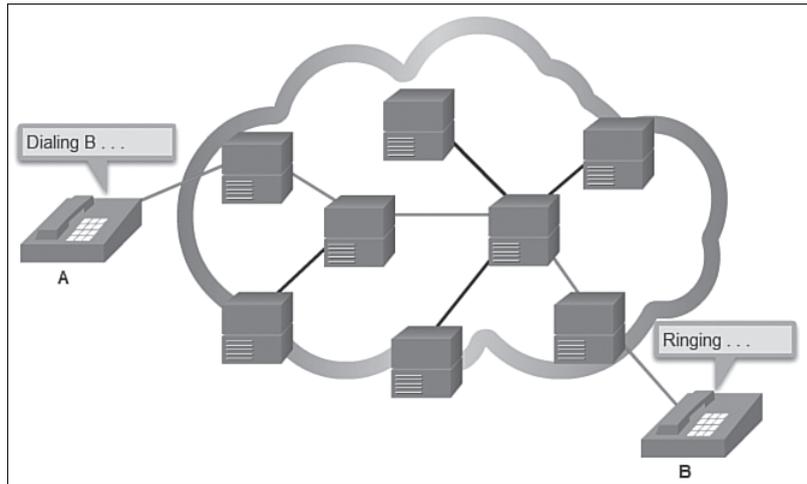
Figure 2-9   Circuit-Switched Connection

As an example, when a subscriber makes a telephone call, the dialed number is used to set switches in the exchanges along the route of the call so that there is a continuous circuit from the caller to the called party. Because of the switching operation used to establish the circuit, the telephone system is called a circuit-switched network. If the telephones are replaced with modems, then the switched circuit is able to carry computer data.

If the circuit carries computer data, the usage of this fixed capacity may not be efficient. For example, if the circuit is used to access the Internet, there is a burst of activity on the circuit while a web page is transferred. This could be followed by no activity while the user reads the page, and then another burst of activity while the next page is transferred. This variation in usage between none and maximum is typical of computer network traffic. Because the subscriber has sole use of the fixed capacity allocation, switched circuits are generally an expensive way of moving data.

The two most common types of circuit-switched WAN technologies are the public switched telephone network (PSTN) and the *Integrated Services Digital Network (ISDN)*.

Video 2.1.2.4: Circuit-Switched Network

Video

Go to the course and play the animation to see how a circuit-switch network connects host A to host B.

Packet-Switched Networks (2.1.2.5)

In contrast to circuit switching, packet switching splits traffic data into packets that are routed over a shared network. Packet-switching networks do not require a circuit to be established, and they allow many pairs of nodes to communicate over the same channel.

The routers in a *packet-switched network (PSN)* determine the links that packets must be sent over based on the addressing information in each packet. The following are two approaches to this link determination:

- **Connectionless systems:** Full addressing information must be carried in each packet. Each router must evaluate the address to determine where to send the packet. An example of a connectionless system is the Internet.

- **Connection-oriented systems:** The network predetermines the route for a packet, and each packet only has to carry an identifier. The router determines the onward route by looking up the identifier in tables held in memory. The set of entries in the tables identifies a particular route or circuit through the system. When the circuit is established temporarily while a packet is traveling through it, and then breaks down again, it is called a *virtual circuit (VC)*. An example of a connection-oriented system is Frame Relay. In the case of Frame Relay, the identifiers used are called data-link connection identifiers (DLCIs).

Because the internal links between the switches are shared between many users, the cost of packet switching is lower than that of circuit-switching. However, delays (latency) and variability of delay (jitter) are greater in packet-switched networks than in circuit-switched networks. This is because the links are shared and because packets must be entirely received at one switch before moving to the next. Despite the latency and jitter inherent in shared networks, modern technology allows satisfactory transport of voice and video communications on these networks.

Video

Video 2.1.2.5: Packet-Switched Network

Go to the course and play the animation to see how a packet-switch network connects host A to host B. In the animation, SRV1 is sending data to SRV2. As the packet traverses the provider network, it arrives at the second provider switch. The packet is added to the queue and forwarded after the other packets in the queue have been forwarded. Eventually, the packet reaches SRV2.

Interactive Graphic

Activity 2.1.2.6: Identify WAN Terminology

Go to the course online to perform this practice activity.

Selecting a WAN Technology (2.2)

Corporate networks can be interconnected using private WAN infrastructures and public WAN infrastructures. This section discusses both types of infrastructures.

WAN Link Connection Options (2.2.1.1)

There are several WAN access connection options that ISPs can use to connect the local loop to the enterprise edge. These WAN access options differ in technology, speed, and cost. Each has distinct advantages and disadvantages. Familiarity with these technologies is an important part of network design.

As summarized in Figure 2-10, an enterprise can get WAN access over a

- *Private WAN infrastructure*: Service providers may offer dedicated point-to-point leased lines, circuit-switched links, such as PSTN or ISDN, and packet-switched links, such as Ethernet WAN, ATM, or Frame Relay.

- *Public WAN infrastructure*: Service provider may offer broadband Internet access using digital subscriber line (DSL), cable, and satellite access. Broadband connection options are typically used to connect small offices and telecommuting employees to a corporate site over the Internet. Data traveling between corporate sites over the public WAN infrastructure should be protected using VPNs.
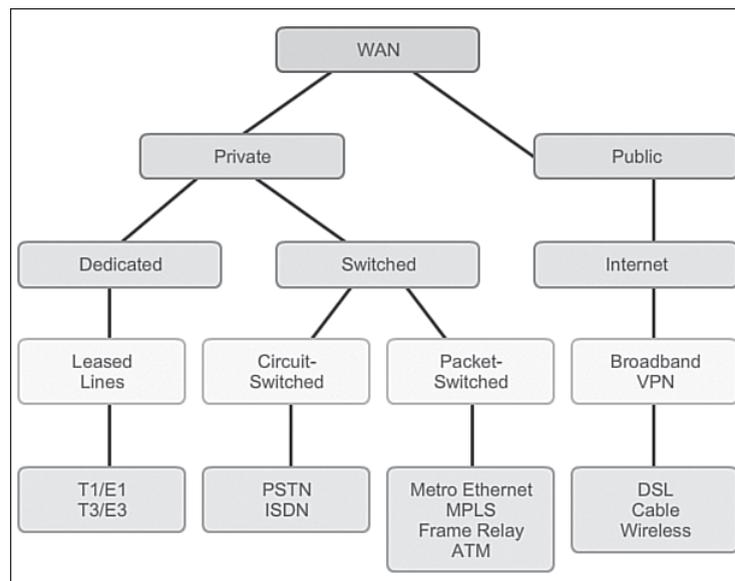
Figure 2-10   WAN Access Options

The topology in Figure 2-11 illustrates some of these WAN access technologies.
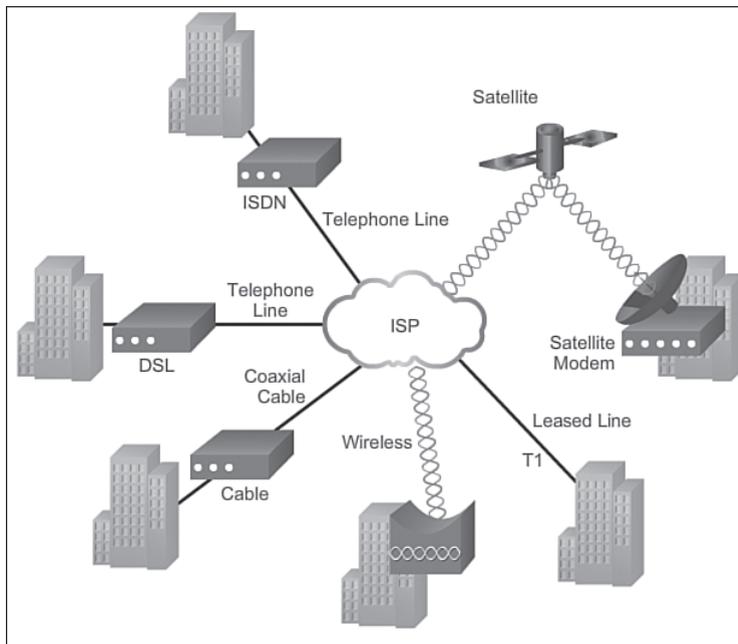
Figure 2-11   WAN Access Technologies

Service Provider Network Infrastructure (2.2.1.2)

When a WAN service provider receives data from a client at a site, it must forward the data to the remote site for final delivery to the recipient. In some cases, the remote site may be connected to the same service provider as the originating site. In other cases, the remote site may be connected to a different ISP, and the originating ISP must pass the data to the connecting ISP.

Long-range communications are usually those connections between ISPs or between branch offices in very large companies.

Service provider networks are complex. They consist mostly of high-bandwidth fiber-optic media, using either the *Synchronous Optical Networking (SONET)* or *Synchronous Digital Hierarchy (SDH)* standard. These standards define how to transfer multiple data, voice, and video traffic over optical fiber using lasers or *light-emitting diodes (LEDs)* over great distances.

Note

SONET is an American-based ANSI standard, while SDH is a European-based ETSI and ITU standard. Both are essentially the same and, therefore, often listed as SONET/SDH.

A newer fiber-optic media development for long-range communications is called *dense wavelength-division multiplexing (DWDM)*. DWDM multiplies the amount of bandwidth that a single strand of fiber can support. As illustrated in Figure 2-12, DWDM assigns incoming signals specific color wavelengths. These signals are transmitted over the fiber-optic cable to the end device, which then separates the traffic accordingly.
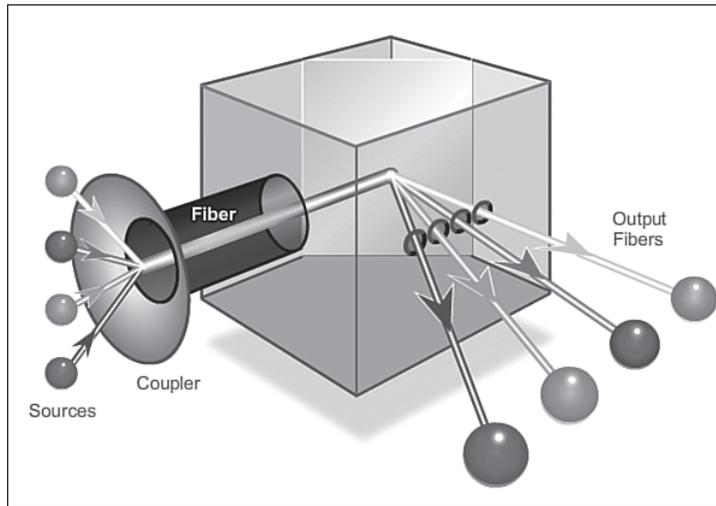
Figure 2-12   DWDM Concept

DWDM circuits are used in all modern submarine communications cable systems and other long-haul circuits.

Specifically, DWDM

- Enables bidirectional communications over one strand of fiber

- Assigns incoming optical signals to specific wavelengths of light (i.e., frequencies)

- Each channel is capable of carrying a 10-Gbps multiplexed signal

- Can multiplex more than 80 different channels of data (i.e., wavelengths) onto a single fiber

- Can amplify these wavelengths to boost the signal strength

- Supports SONET and SDH standards

Interactive Graphic

Activity 2.2.1.3: Classify WAN Access Options

Go to the course online to perform this practice activity.

Private WAN Infrastructures (2.2.2)

In this topic, private WAN infrastructures are discussed including leased lines, dialup access, ISDN, Frame Relay, ATM, MPLS, and Ethernet WANs, and VSAT.

Leased Lines (2.2.2.1)

When permanent dedicated connections are required, a point-to-point link is used to provide a pre-established WAN communications path from the customer premises to the provider network. Point-to-point lines are usually leased from a service provider and are called *leased lines*.

Leased lines have existed since the early 1950s, and for this reason are referred to by different names, such as leased circuits, serial link, serial line, point-to-point link, and T1/E1 or T3/E3 lines. The term leased line refers to the fact that the organization pays a monthly lease fee to a service provider to use the line. Leased lines are available in different capacities and are generally priced based on the bandwidth required and the distance between the two connected points.

In North America, service providers use the T-carrier system to define the digital transmission capability of a serial copper media link, while Europe uses the E-carrier system, as shown in Figure 2-13.
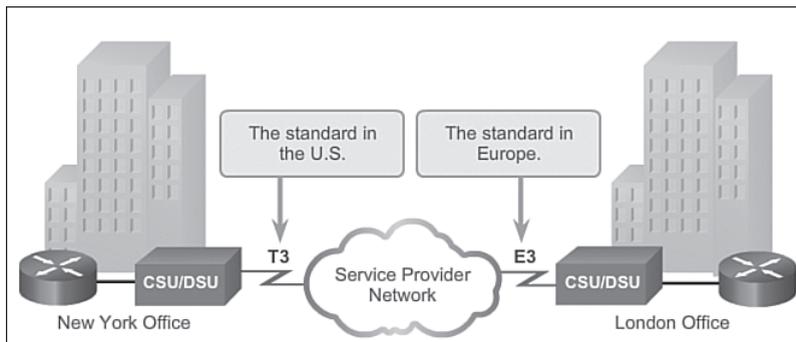
Figure 2-13   Sample Leased Line Topology

For instance, a T1 link supports 1.544 Mbps, an E1 supports 2.048 Mbps, a T3 supports 43.7 Mbps, and an E3 connection supports 34.368 Mbps. Optical Carrier (OC) transmission rates are used to define the digital transmitting capacity of a fiber-optic network.

The advantages of leased lines include

- **Simplicity:** Point-to-point communication links require minimal expertise to install and maintain.

- **Quality**: Point-to-point communication links usually offer high service quality, if they have adequate bandwidth. The dedicated capacity removes latency or jitter between the endpoints.

- **Availability**: Constant availability is essential for some applications, such as e-commerce. Point-to-point communication links provide permanent, dedicated capacity, which is required for VoIP or Video over IP.

The disadvantages of leased lines include

- **Cost**: Point-to-point links are generally the most expensive type of WAN access. The cost of leased line solutions can become significant when they are used to connect many sites over increasing distances. In addition, each endpoint requires an interface on the router, which increases equipment costs.

- **Limited flexibility**: WAN traffic is often variable, and leased lines have a fixed capacity, so that the bandwidth of the line seldom matches the need exactly. Any change to the leased line generally requires a site visit by ISP personnel to adjust capacity.

The Layer 2 protocol is usually HDLC or PPP.

Dialup (2.2.2.2)

Dialup WAN access may be required when no other WAN technology is available. For example, a remote location could use a modem and analog dialed telephone lines to provide low-capacity and dedicated switched connections. Dialup access is suitable when intermittent, low-volume data transfers are needed.

Traditional telephony uses a copper cable for the local loop to connect the telephone handset in the subscriber premises to the CO. The signal on the local loop during a call is a continuously varying electronic signal that is a translation of the subscriber voice into an analog signal.

Traditional local loops can transport binary computer data through the voice telephone network using a modem. The modem modulates the binary data into an analog signal at the source and demodulates the analog signal to binary data at the destination. The physical characteristics of the local loop and its connection to the PSTN limit the rate of the signal to less than 56 Kbps.

For small businesses, these relatively low-speed dialup connections are adequate for the exchange of sales figures, prices, routine reports, and email. Using automatic dialup at night or on weekends for large file transfers and data backup can take advantage of lower off-peak tariffs (toll charges). Tariffs are based on the distance between the endpoints, time of day, and the duration of the call.

The advantages of modem and analog lines are simplicity, availability, and low implementation cost. The disadvantages are the low data rates and a relatively long connection time. The dedicated circuit has little delay or jitter for point-to-point traffic, but voice or video traffic does not operate adequately at these low bit rates.

Figure 2-14 displays a sample topology of two remote sites interconnecting with dialup modems.

WAN built with an on demand connection using a modem and the voice telephone network.
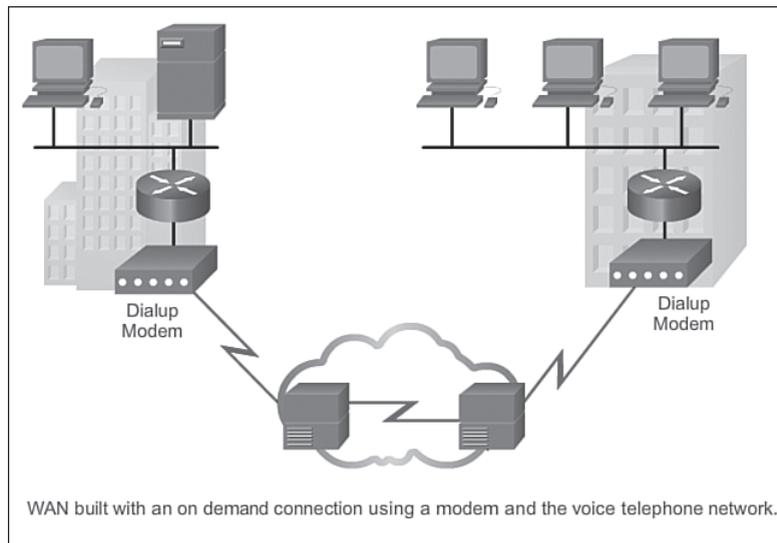
Figure 2-14   Sample Dialup Topology

Note

Although very few enterprises support dialup access, it is still a viable solution for remote areas with limited WAN access options.

ISDN (2.2.2.3)

Integrated Services Digital Network (ISDN) is a circuit-switching technology that enables the local loop of a PSTN to carry digital signals, resulting in higher-capacity switched connections.

ISDN changes the internal connections of the PSTN from carrying analog signals to time-division multiplexed (TDM) digital signals. TDM allows two or more signals, or bit streams, to be transferred as subchannels in one communication channel. The signals appear to transfer simultaneously; but physically, the signals are taking turns on the channel.

Figure 2-15 displays a sample ISDN topology. The ISDN connection may require a terminal adapter (TA), which is a device used to connect ISDN Basic Rate Interface (BRI) connections to a router.
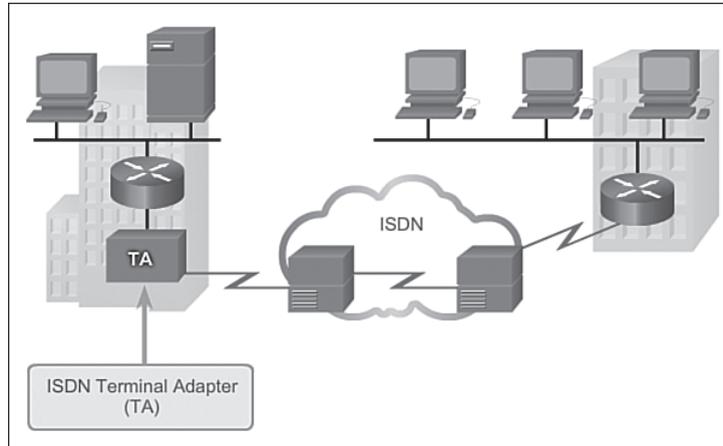
Figure 2-15   Sample ISDN Topology

ISDN turns the local loop into a TDM digital connection. This change enables the local loop to carry digital signals that result in higher-capacity switched connections. The connection uses 64-Kbps bearer channels (B) for carrying voice or data and a signaling delta channel (D) for call setup and other purposes.

There are two types of ISDN interfaces:

- *Basic Rate Interface (BRI)*: ISDN BRI is intended for the home and small enterprise and provides two 64-Kbps B channels and one 16-Kbps D channel. The BRI D channel is designed for control and often underused, because it has only two B channels to control (Figure 2-16).

Figure 2-16   ISDN BRI

- *Primary Rate Interface (PRI)*: ISDN is also available for larger installations. In North America, PRI delivers 23 B channels with 64 Kbps and 1 D channel with 64 Kbps for a total bit rate of up to 1.544 Mbps. This includes some additional

overhead for synchronization. In Europe, Australia, and other parts of the world, ISDN PRI provides 30 B channels and 1 D channel, for a total bit rate of up to 2.048 Mbps, including synchronization overhead (see Figure 2-17).
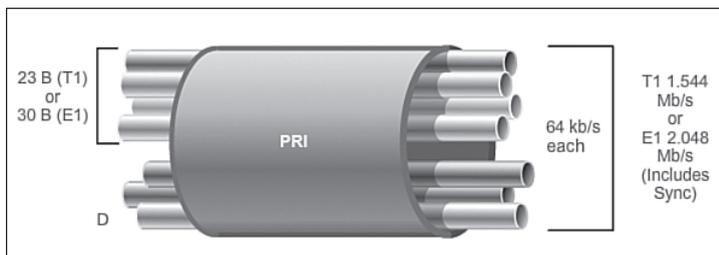
Figure 2-17   ISDN PRI

BRI has a call setup time that is less than a second, and the 64-Kbps B channel provides greater capacity than an analog modem link. If greater capacity is required, a second B channel can be activated to provide a total of 128 Kbps. Although inadequate for video, this permits several simultaneous voice conversations in addition to data traffic.

Another common application of ISDN is to provide additional capacity as needed on a leased line connection. The leased line is sized to carry average traffic loads while ISDN is added during peak demand periods. ISDN is also used as a backup if the leased line fails. ISDN tariffs are based on a per-B-channel basis and are similar to those of analog voice connections.

With PRI ISDN, multiple B channels can be connected between two endpoints. This allows for videoconferencing and high-bandwidth data connections with no latency or jitter. However, multiple connections can be very expensive over long distances.

Note

Although ISDN is still an important technology for telephone service provider networks, it is declining in popularity as an Internet connection option with the introduction of high-speed DSL and other broadband services.
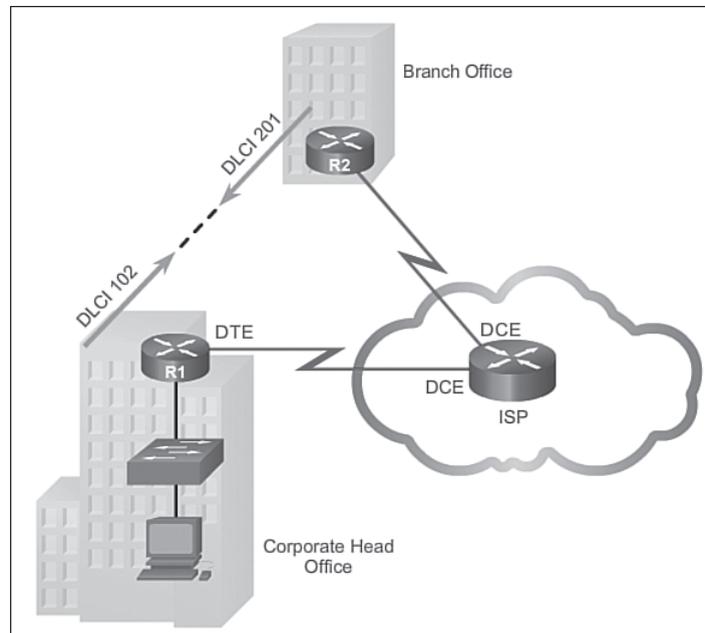
Frame Relay (2.2.2.4)

Frame Relay is a simple Layer 2 nonbroadcast multiaccess (NBMA) WAN technology used to interconnect enterprise LANs. A single router interface can be used to connect to multiple sites using PVCs. PVCs are used to carry both voice and data traffic between a source and destination, and support data rates up to 4 Mbps, with some providers offering even higher rates.

An edge router only requires a single interface, even when multiple virtual circuits (VCs) are used. The short-leased line to the Frame Relay network edge allows cost-effective connections between widely scattered LANs.

Frame Relay creates PVCs, which are uniquely identified by a data-link connection identifier (DLCI). The PVCs and DLCIs ensure bidirectional communication from one DTE device to another.

For instance, in the example in Figure 2-18 R1 will use DLCI 102 to reach R2, while R2 will use DLCI 201 to reach R1.

Figure 2-18   Sample Frame Relay Topology

ATM (2.2.2.5)

Asynchronous Transfer Mode (ATM) technology is capable of transferring voice, video, and data through private and public networks. It is built on a cell-based architecture rather than on a frame-based architecture. ATM cells are always a fixed length of 53 bytes. The ATM cell contains a 5-byte ATM header followed by 48 bytes of ATM payload. Small fixed-length cells are well-suited for carrying voice and video traffic because this traffic is intolerant of delay. Video and voice traffic do not have to wait for larger data packets to be transmitted.

The 53-byte ATM cell is less efficient than the bigger frames and packets of Frame Relay. Furthermore, the ATM cell has at least 5 bytes of overhead for each 48-byte payload. When the cell is carrying segmented network layer packets, the overhead is

higher because the ATM switch must be able to reassemble the packets at the destination. A typical ATM line needs almost 20 percent greater bandwidth than Frame Relay to carry the same volume of network layer data.

ATM was designed to be extremely scalable and to support link speeds of T1/E1 to OC-12 (622 Mbps) and faster.

ATM offers both PVCs and SVCs, although PVCs are more common with WANs. As with other shared technologies, ATM allows multiple VCs on a single leased-line connection to the network edge.

In the example in Figure 2-19, the ATM switch transmits four different traffic flows consisting of video, VoIP, web, and email.
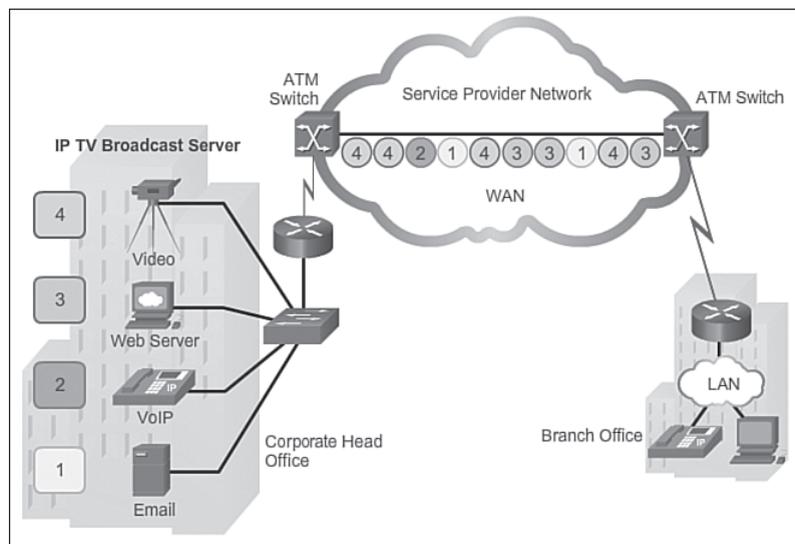

Figure 2-19   Sample ATM Topology

Ethernet WAN (2.2.2.6)

Ethernet was originally developed to be a LAN access technology. At that time however, it really was not suitable as a WAN access technology because the maximum cable length supported was only up to a kilometer. However, newer Ethernet standards using fiber-optic cables have made Ethernet a reasonable WAN access option. For instance, the IEEE 1000BASE-LX standard supports fiber-optic cable lengths of 5 km, while the IEEE 1000BASE-ZX standard supports up to 70 km cable lengths.

Service providers now offer Ethernet WAN service using fiber-optic cabling. The Ethernet WAN service can go by many names, including *Metropolitan Ethernet (MetroE)*, *Ethernet over MPLS (EoMPLS)*, and *Virtual Private LAN Service (VPLS)*.

Figure 2-20 displays a sample Ethernet WAN topology.
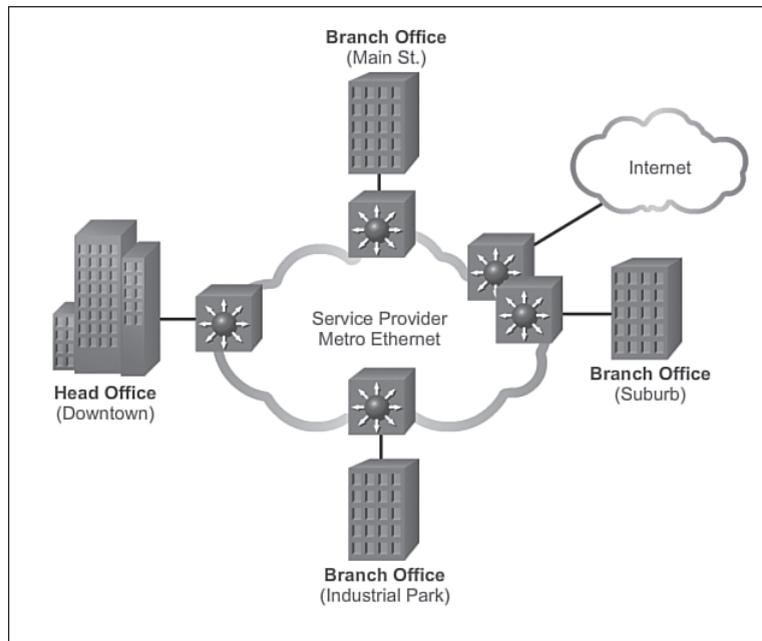
Figure 2-20   Sample Ethernet WAN Topology

Benefits of Ethernet WAN include

- **Reduced expenses and administration:** Ethernet WAN provides a switched, high-bandwidth Layer 2 network capable of managing data, voice, and video all on the same infrastructure. This characteristic increases bandwidth and eliminates expensive conversions to other WAN technologies. The technology enables businesses to inexpensively connect numerous sites, in a metropolitan area, to each other and to the Internet.

- **Easy integration with existing networks:** Ethernet WAN connects easily to existing Ethernet LANs, reducing installation costs and time.

- **Enhanced business productivity:** Ethernet WAN enables businesses to take advantage of productivity-enhancing IP applications that are difficult to implement on TDM or Frame Relay networks, such as hosted IP communications, VoIP, and streaming and broadcast video.

Note

Ethernet WANs have gained in popularity and are now commonly being used to replace the traditional Frame Relay and ATM WAN links.

MPLS (2.2.2.7)

Multiprotocol Label Switching (MPLS) is a multiprotocol high-performance WAN technology that directs data from one router to the next based on short path labels rather than IP network addresses.

MPLS has several defining characteristics. It is multiprotocol, meaning it has the ability to carry any payload including IPv4, IPv6, Ethernet, ATM, DSL, and Frame Relay traffic. It uses labels that tell a router what to do with a packet. The labels identify paths between distant routers rather than endpoints, and while MPLS actually routes IPv4 and IPv6 packets, everything else is switched.

MPLS is a service provider technology. Leased lines deliver bits between sites, and Frame Relay and Ethernet WAN deliver frames between sites. However, MPLS can deliver any type of packet between sites. MPLS can encapsulate packets of various network protocols. It supports a wide range of WAN technologies, including T-carrier / E-carrier links, Carrier Ethernet, ATM, Frame Relay, and DSL.

The sample topology in Figure 2-21 illustrates how MPLS is used.
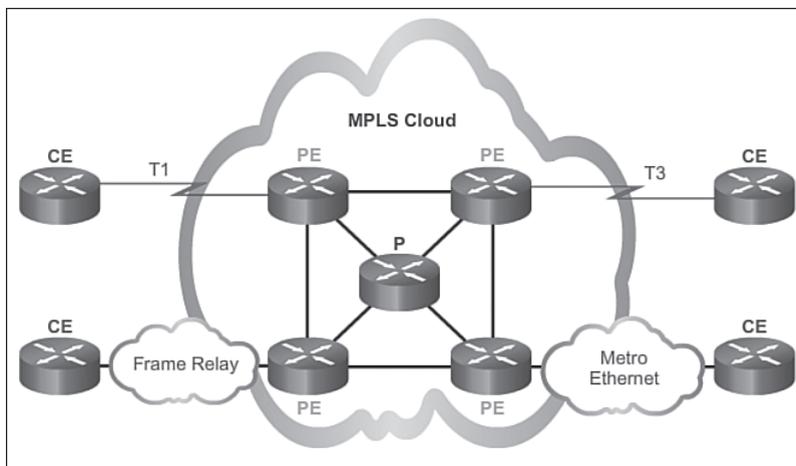
Figure 2-21   Sample MPLS Topology

Notice that the different sites can connect to the MPLS cloud using different access technologies. In the figure, CE refers to the customer edge, PE is the provider edge router, which adds and removes labels, while P is an internal provider router, which switches MPLS labeled packets.

**Note**

MPLS is primarily a service provider WAN technology.

VSAT (2.2.2.8)

All private WAN technologies discussed so far used either copper or fiber-optic media. What if an organization needs connectivity in a remote location where there are no service providers that offer WAN service?

Very small aperture terminal (VSAT) is a solution that creates a private WAN using satellite communications. A VSAT is a small satellite dish similar to those used for home Internet and TV. VSATs create a private WAN while providing connectivity to remote locations.

Specifically, a router connects to a satellite dish that is pointed to a service provider's satellite in a geosynchronous orbit in space. The signals must travel approximately 35,786 km (22,236 miles) to the satellite and back.

The example in Figure 2-22 displays a VSAT dish on the roofs of the buildings communicating with a satellite dish thousands of kilometers away in space.
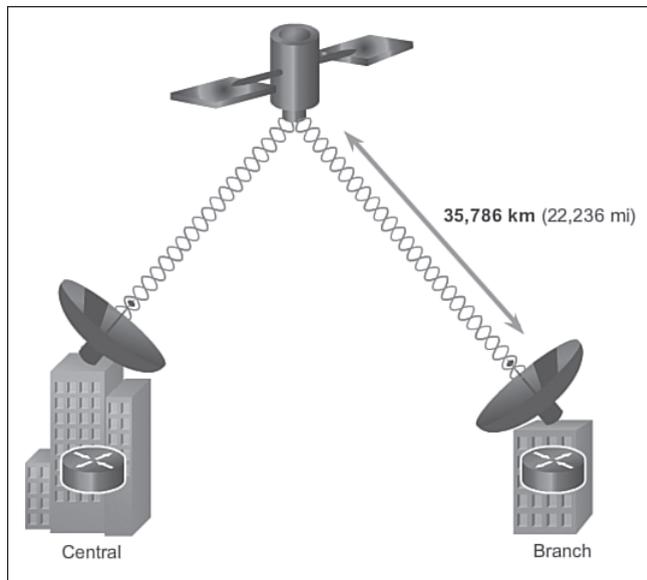
Figure 2-22   Sample VSAT Topology

Activity 2.2.2.9: Identify Private WAN Infrastructure Terminology

Go to the course online to perform this practice activity.

Public WAN Infrastructure (2.2.3)

In this topic, public WAN infrastructures are discussed, including DSL, cable, wireless, 3G/4G cellular, as well as the need to secure data using site-to-site VPNs and remote-access VPNs.

DSL (2.2.3.1)

DSL technology is an always-on connection technology that uses existing twisted-pair telephone lines to transport high-bandwidth data, and provides IP services to subscribers. A *DSL modem* converts an Ethernet signal from the user device to a DSL signal, which is transmitted to the central office.

Multiple DSL subscriber lines are multiplexed into a single high-capacity link using a *DSL access multiplexer (DSLAM)* at the provider location. DSLAMs incorporate TDM technology to aggregate many subscriber lines into a single medium, generally a T3 (DS3) connection. Current DSL technologies use sophisticated coding and modulation techniques to achieve fast data rates.

There is a wide variety of DSL types, standards, and emerging standards. DSL is now a popular choice for enterprise IT departments to support home workers. Generally, a subscriber cannot choose to connect to an enterprise network directly, but must first connect to an ISP, and then an IP connection is made through the Internet to the enterprise. Security risks are incurred in this process, but can be mediated with security measures.

The topology in Figure 2-23 displays a sample DSL WAN connection.
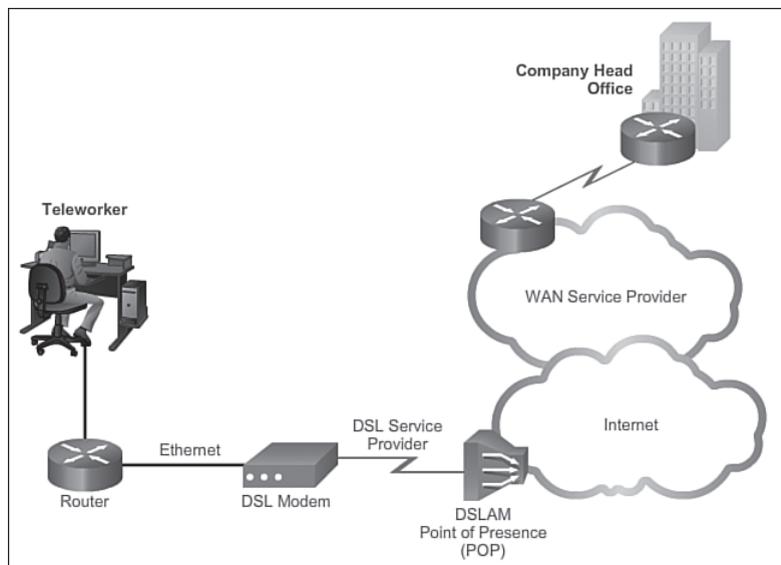
Figure 2-23   Sample DSL Topology

Cable (2.2.3.2)

Coaxial cable is widely used in urban areas to distribute television signals. Network access is available from many cable television providers. This allows for greater bandwidth than the conventional telephone local loop.

Cable modems provide an always-on connection and a simple installation. A subscriber connects a computer or LAN router to the cable modem, which translates the digital signals into the broadband frequencies used for transmitting on a cable television network. The local cable TV office, which is called the cable *headend*, contains the computer system and databases needed to provide Internet access. The most important component located at the headend is the *cable modem termination system (CMTS)*, which sends and receives digital cable modem signals on a cable network and is necessary for providing Internet services to cable subscribers.

Cable modem subscribers must use the ISP associated with the service provider. All the local subscribers share the same cable bandwidth. As more users join the service, available bandwidth may be below the expected rate.

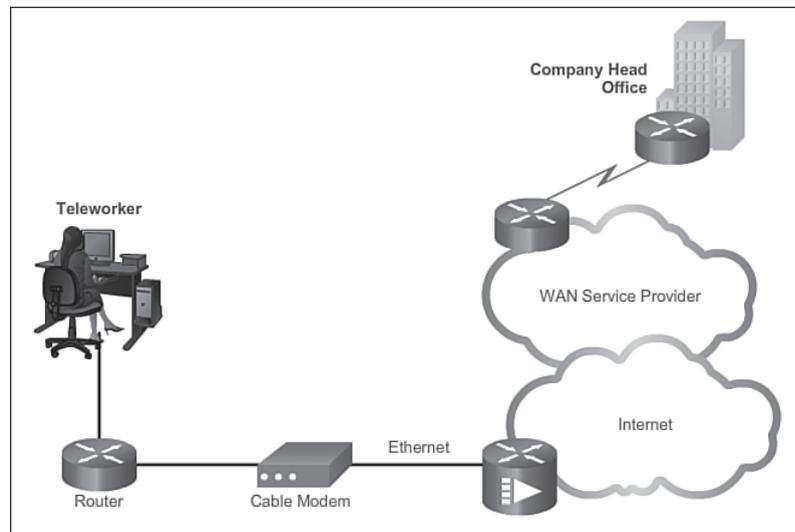The topology in Figure 2-24 displays a sample cable WAN connection.


Figure 2-24   Sample Cable Topology

Wireless (2.2.3.3)

Wireless technology uses the unlicensed radio spectrum to send and receive data. The unlicensed spectrum is accessible to anyone who has a wireless router and wireless technology in the device they are using.

Until recently, one limitation of wireless access has been the need to be within the local transmission range (typically less than 100 feet) of a wireless router or a wireless modem that has a wired connection to the Internet. The following new developments in broadband wireless technology are changing this situation:

- *Municipal Wi-Fi*: Many cities have begun setting up municipal wireless networks. Some of these networks provide high-speed Internet access for free or for substantially less than the price of other broadband services. Others are for city use only, allowing police and fire departments and other city employees to do certain aspects of their jobs remotely. To connect to a municipal Wi-Fi, a subscriber typically needs a wireless modem, which provides a stronger radio and directional antenna than conventional wireless adapters. Most service providers provide the necessary equipment for free or for a fee, much like they do with DSL or cable modems.

- *WiMAX*: Worldwide Interoperability for Microwave Access (WiMAX) is a new technology that is just beginning to come into use. It is described in the IEEE standard 802.16. WiMAX provides high-speed broadband service with wireless access and provides broad coverage like a cell phone network rather than through small Wi-Fi hotspots. WiMAX operates in a similar way to Wi-Fi, but at higher speeds, over greater distances, and for a greater number of users. It uses a network of WiMAX towers that are similar to cell phone towers. To access a WiMAX network, subscribers must subscribe to an ISP with a WiMAX tower within 30 miles of their location. They also need some type of WiMAX receiver and a special encryption code to get access to the base station.

- *Satellite Internet*: Typically used by rural users where cable and DSL are not available. A VSAT provides two-way (upload and download) data communications. The upload speed is about one-tenth of the 500 Kbps download speed. Cable and DSL have higher download speeds, but satellite systems are about 10 times faster than an analog modem. To access satellite Internet services, subscribers need a satellite dish, two modems (uplink and downlink), and coaxial cables between the dish and the modem.

Figure 2-25 displays an example of a WiMAX network.
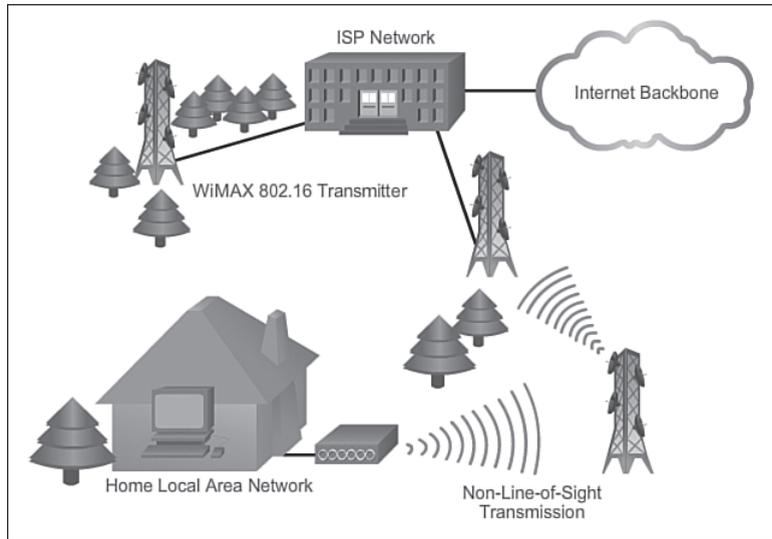
Figure 2-25   Sample Wireless Topology

3G/4G Cellular (2.2.3.4)

Increasingly, cellular service is another wireless WAN technology being used to connect users and remote locations where no other WAN access technology is available. Many users with smartphones and tablets can use cellular data to email, surf the Web, download apps, and watch videos.

Phones, tablet computers, laptops, and even some routers can communicate through to the Internet using cellular technology. As shown in Figure 2-26, these devices use radio waves to communicate through a nearby mobile phone tower.
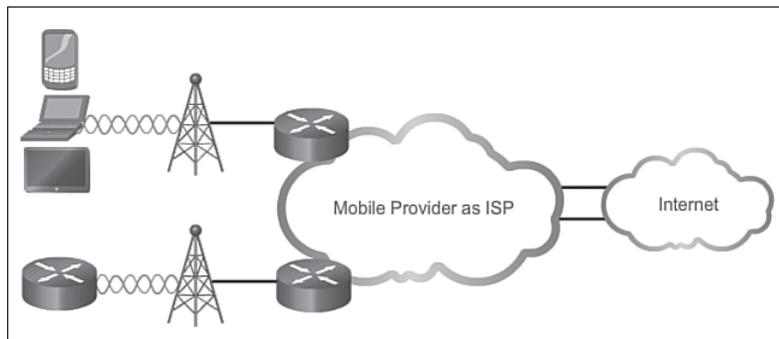
Figure 2-26   Sample Cellular Topology

The device has a small radio antenna, and the provider has a much larger antenna sitting at the top of a tower somewhere within miles of the phone.

Common cellular industry terms include

- *3G/4G Wireless*: Abbreviation for third-generation and fourth-generation cellular access. These technologies support wireless Internet access.

- *Long Term Evolution (LTE)*: Refers to a newer and faster technology and is considered to be part of fourth generation (4G) technology.

VPN Technology (2.2.3.5)

Security risks are incurred when a teleworker or a remote office worker uses broadband services to access the corporate WAN over the Internet. To address security concerns, broadband services provide capabilities for using VPN connections to a VPN server, which is typically located at the corporate site.

A VPN is an encrypted connection between private networks over a public network, such as the Internet. Instead of using a dedicated Layer 2 connection, such as a leased line, a VPN uses virtual connections called VPN tunnels, which are routed through the Internet from the private network of the company to the remote site or employee host.

Benefits of VPN include the following:

- **Cost savings:** VPNs enable organizations to use the global Internet to connect remote offices and remote users to the main corporate site, thus eliminating expensive dedicated WAN links and modem banks.

- **Security:** VPNs provide the highest level of security by using advanced encryption and authentication protocols that protect data from unauthorized access.

- **Scalability:** Because VPNs use the Internet infrastructure within ISPs and devices, it is easy to add new users. Corporations are able to add large amounts of capacity without adding significant infrastructure.

- **Compatibility with broadband technology:** VPN technology is supported by broadband service providers such as DSL and cable, so mobile workers and telecommuters can take advantage of their home high-speed Internet service to access their corporate networks. Business-grade high-speed broadband connections can also provide a cost-effective solution for connecting remote offices.

There are two types of VPN access:

- *Site-to-site VPNs*: Site-to-site VPNs connect entire networks to each other; for example, they can connect a branch office network to a company headquarters network, as shown in Figure 2-27. Each site is equipped with a VPN gateway, such as a router, firewall, VPN concentrator, or security appliance. In the figure, a remote branch office uses a site-to-site-VPN to connect with the corporate head office.
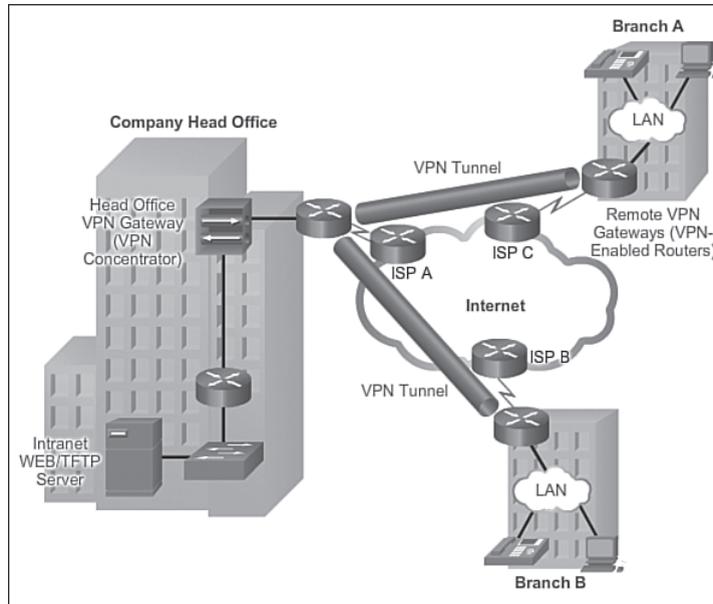
Figure 2-27   Sample Site-to-Site VPN Topology

- *Remote-access VPNs*: Remote-access VPNs enable individual hosts, such as tele-commuters, mobile users, and extranet consumers, to access a company network securely over the Internet. Each host (Teleworker 1 and Teleworker 2) typically has VPN client software loaded or uses a web-based client, as shown in Figure 2-28.
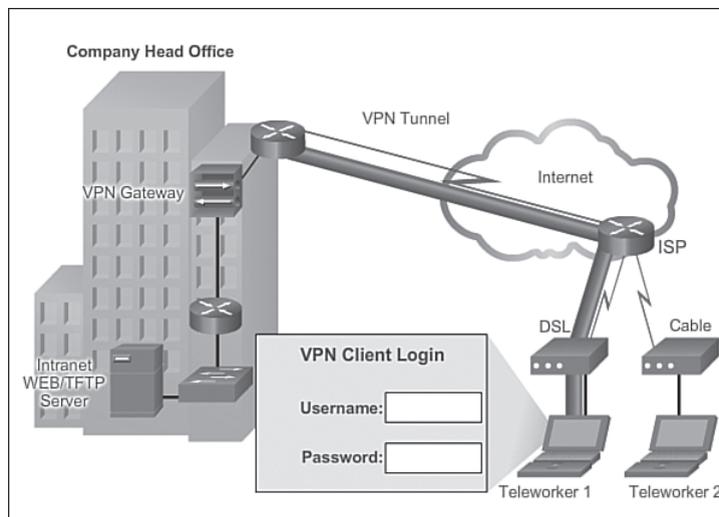
Figure 2-28   Sample Remote-Access VPN Topology

Activity 2.2.3.6: Identify Public WAN Infrastructure Terminology

Go to the course online to perform this practice activity.

Selecting WAN Services (2.2.4)

Many factors influence the choice of service provider. This topic discusses how the purpose of the WAN, the geographic scope of the WAN, and the traffic requirements all factor in when choosing service providers.

Choosing a WAN Link Connection (2.2.4.1, 2.2.4.2)

There are many important factors to consider when choosing an appropriate WAN connection. For a network administrator to decide which WAN technology best meets the requirements of their specific business, they must answer the following questions:

What Is the Purpose of the WAN?

Considerations include

- Will the enterprise connect local branches in the same city area, connect remote branches, or connect to a single branch?

- Will the WAN be used to connect internal employees, or external business partners and customers, or all three?

- Will the enterprise connect to customers, connect to business partners, connect to employees, or some combination of these?

- Will the WAN provide authorized users limited or full access to the company intranet?

What Is the Geographic Scope?

Considerations include

- Is the WAN local, regional, or global?

- Is the WAN one to one (single branch), one to many branches, or many to many (distributed)?

What Are the Traffic Requirements?

Considerations include

- What type of traffic must be supported (data only, VoIP, video, large files, streaming files)? This determines the quality and performance requirements.

- What volume of traffic type (voice, video, or data) must be supported for each destination? This determines the bandwidth capacity required for the WAN connection to the ISP.

- What quality of service is required? This may limit the choices. If the traffic is highly sensitive to latency and jitter, eliminate any WAN connection options that cannot provide the required quality.

- What are the security requirements (data integrity, confidentiality, and security)? These are important factors if the traffic is of a highly confidential nature, or if it provides essential services, such as emergency response.

In addition to gathering information about the scope of the WAN, the administrator must also determine

- **Should the WAN use a private or public infrastructure?** A private infrastructure offers the best security and confidentiality, whereas the public Internet infrastructure offers the most flexibility and lowest ongoing expense. The choice depends on the purpose of the WAN, the types of traffic it carries, and available operating budget. For example, if the purpose is to provide a nearby branch with high-speed, secure services, a private dedicated or switched connection may be best. If the purpose is to connect many remote offices, a public WAN using the Internet may be the best choice. For distributed operations, a combination of options may be the solution.

- **For a private WAN, should it be dedicated or switched?** Real-time high-volume transactions have special requirements that could favor a dedicated line, such as traffic flowing between the data center and the corporate head office. If the enterprise is connecting to a local single branch, a dedicated leased line could be used. However, that option would become very expensive for a WAN connecting multiple offices. In that case, a switched connection might be better.

- **For a public WAN, what type of VPN access is required?** If the purpose of the WAN is to connect a remote office, a site-to-site VPN may be the best choice. To connect teleworkers or customers, remote-access VPNs are a better option. If the WAN is serving a mixture of remote offices, teleworkers, and authorized customers, such as a global company with distributed operations, a combination of VPN options may be required.

■ **Which connection options are available locally?** In some areas, not all WAN connection options are available. In this case, the selection process is simplified, although the resulting WAN may provide less-than-optimal performance. For example, in a rural or remote area, the only option may be VSAT or cellular access.

■ **What is the cost of the available connection options?** Depending on the option chosen, the WAN can be a significant ongoing expense. The cost of a particular option must be weighed against how well it meets the other requirements. For example, a dedicated leased line is the most expensive option, but the expense may be justified if it is critical to ensure secure transmission of high volumes of real-time data. For less-demanding applications, a less-expensive switched or Internet connection option may be more suitable.

Using the guidelines described here, as well as those described by the Cisco Enterprise Architecture, a network administrator should be able to choose an appropriate WAN connection to meet the requirements of different business scenarios.

Lab 2.2.4.3: Researching WAN Technologies

In this lab, you will complete the following objectives:

■ Part 1: Investigate Dedicated WAN Technologies and Providers

■ Part 2: Investigate a Dedicated Leased Line Service Provider in Your Area

Summary (2.3)

Class Activity 2.3.1.1: WAN Device Modules

Your medium-size company is upgrading its network. To make the most of the equipment currently in use, you decide to purchase WAN modules instead of new equipment.

All branch offices use either Cisco 1900 or 2911 series ISRs. You will be updating these routers in several locations. Each branch has its own ISP requirements to consider.

To update the devices, focus on the following WAN modules access types:

- Ethernet
- Broadband
- T1/E1 and ISDN PRI
- BRI
- Serial
- T1 and E1 trunk voice and WAN
- Wireless LANs and WANs

A business can use private lines or the public network infrastructure for WAN connections. A public infrastructure connection can be a cost-effective alternative to a private connection between LANs, as long as security is also planned.

WAN access standards operate at Layers 1 and 2 of the OSI model, and are defined and managed by the TIA/EIA, ISO, and IEEE. A WAN may be circuit switched or packet switched.

There is common terminology used to identify the physical components of WAN connections and who, the service provider or the customer, is responsible for which components.

Service provider networks are complex and the service provider's backbone networks consist primarily of high-bandwidth fiber-optic media. The device used for interconnection to a customer is specific to the WAN technology that is implemented.

Permanent, dedicated, point-to-point connections are provided by using leased lines. Dialup access, although slow, is still viable for remote areas with limited WAN options. Other private connection options include ISDN, Frame Relay, ATM, Ethernet WAN, MPLS, and VSAT.

Public infrastructure connections include DSL, cable, wireless, and 3G/4G cellular. Security over public infrastructure connections can be provided by using remote-access or site-to-site virtual private networks (VPNs).

Practice

The following activities provide practice with the topics introduced in this chapter. The Labs and Class Activities are available in the companion *Connecting Networks Lab Manual* (978-1-58713-331-2).

Class Activities

Class Activity 2.0.1.2: Branching Out

Class Activity 2.3.1.1: WAN Device Modules

Labs

Lab 2.2.4.3: Researching WAN Technologies

Check Your Understanding Questions

Complete all the review questions listed here to test your understanding of the topics and concepts in this chapter. The appendix, "Answers to the 'Check Your Understanding' Questions," lists the answers.

1. A broadband service such as DSL available through a local Internet service provider is suitable for what type of organization?

    A. A small company with 10 employees that uses a single LAN to share information

    B. A medium-size company with 500 employees that uses multiple LANs to share information

    C. A large company with 2,000 employees, in multiple locations and in a multi-LAN environment.

2. Which device is a data terminal equipment?

    A. Cable modem

    B. CSU/DSU

    C. Dialup modem

    D. DSL modem

    E. Router

3. Which two devices are used when digital leased lines interconnect a client with a provider? (Choose two.)

   A. Access server
   B. Channel service unit (CSU)
   C. Data service unit (DSU)
   D. Dialup modem
   E. Layer 2 switch
   F. Router

4. Which statements are true regarding connection-orientated packet-switched networks? (Choose three.)

   A. A virtual circuit is created for the duration of the packet delivery.
   B. Each packet has to carry only an identifier.
   C. Ethernet is an example.
   D. Full addressing information must be carried in each data packet.
   E. The Internet is an example.
   F. The network predetermines the route for each packet.

5. Which technology supports long distance SONET and SDH connections using fiber-optic media?

   A. ATM
   B. DSL
   C. DWDM
   D. Frame Relay
   E. ISDN
   F. MPLS
   G. Municipal Wi-Fi
   H. VPN
   I. VSAT
   J. WiMAX

6. What WAN technology is designed to deliver data, voice, and video simultaneously built on a cell-based architecture?

A. ATM

B. DSL

C. DWDM

D. Frame Relay

E. ISDN

F. MPLS

G. Municipal Wi-Fi

H. VPN

I. VSAT

J. WiMAX

7. ISDN PRI is composed of how many B channels in North America?

A. 2

B. 16

C. 23

D. 30

E. 64

8. The ability to connect securely to a private network over a public network is provided by which WAN technology?

A. ATM

B. DSL

C. DWDM

D. Frame Relay

E. ISDN

F. MPLS

G. VPN

H. VSAT

I. WiMAX

9. What term describes the cabling that connects the customer site to the nearest exchange of the WAN service provider?

    A. CO

    B. DCE

    C. DTE

    D. Local loop

10. Which two statements about a circuit-switched network are true? (Choose two.)

    A. A dedicated secure circuit is established between each pair of communicating nodes.

    B. A connection through the service provider network is established quickly before communications start.

    C. Multiple pairs of nodes can communicate over the same network channel.

    D. The communication costs are lower.