LESSON TEN

HIGH SPEED DIGITAL ACCESS

Broadband Internet access

Specific Objectives

By the end of the lesson the learner should be able to:

(i) Describe LAN Switching
(ii) Describe the WAN technologies
(iii) Compare and contrast DSL to cable MODEM technology

Broadband Internet access, often shortened to just **broadband**, is high-speed Internet access—typically contrasted with dial-up access over a modem.

LAN Switching

Enables dedicated access

– Eliminates collisions and

Increases capacity–

Supports multiple conversations at the same time First of all, it's important to understand the reason that we use LAN switching. Basically, they do this to provide micro-segmentation. Again, micro-segmentation provides dedicated bandwidth for each user on the network. What this is going to do is eliminate collisions in our network, and it's going to effectively increase the capacity for each station connected to the network. It'll also support multiple, simultaneous conversations at any given time, and this will dramatically improve the bandwidth that's available, and it'll dramatically improve the scalability in our network.

LAN Switching operations

A LAN is a high-speed data network that covers a relatively small geographic area. It typically connects workstations, personal computers, printers, servers, and other devices. LANs offer computer users many advantages, including shared access to devices and applications, file exchange between connected users, and communication between users via electronic mail and other applications.

LAN switching is a form of packet switching used in local area networks. Switching technologies are crucial to network design, as they allow traffic to be sent only where it is needed in most cases, using fast, hardware-based methods.

The term Ethernet refers to the family of local-area network (LAN) products covered by the IEEE 802.3 standard that defines what is commonly known as the CSMA/CD protocol. Three data rates are currently defined for operation over optical fiber and twisted-pair cables:

- 10 Mbps-10Base-T Ethernet
- 100 Mbps-Fast Ethernet
- 1000 Mbps-Gigabit Ethernet

10-Gigabit Ethernet is under development and will likely be published as the IEEE 802.3ae supplement to the IEEE 802.3 base standard.

It includes the following topics –

- Ethernet LAN Media and Cable Lengths
- Hubs Bridges and Switches
- Forward and Filter Decision Switching
- Learning MAC Addresses and Frames Flooding
- Spanning Tree Protocol

  Collision Domains and Broadcast Domains

- Virtual LANs VLAN

What is a network switch, and how does it work?
Switches connect network segments, providing full-duplex communication, valuable network performance data and efficient use of network bandwidth.

Networks today are essential for supporting businesses, providing communication, delivering entertainment—the list goes on and on. A fundamental element networks have in common is the network switch, which helps connect devices for the purpose of sharing resources.

What is a network switch?
A network switch is a device that operates at the Data Link layer of the OSi reference model—Layer 2. It takes in packets being sent by devices that are connected to its physical ports and sends them out again, but only through the ports that lead to the devices the packets are intended to reach. They can also operate at the network layer-Layer 3 where routing occurs.

Switches are a common component of networks based on Ethernet, Fiber Channel, Asynchronous Transfer Mode (ATM), among others. In general, though, most switches today use Ethernet.

How does a network switch work?
Once a device is connected to a switch, the switch notes its media access control (MAC) address, a code that's baked into the device's network-interface card (NIC) that attaches to an Ethernet cable that attaches to the switch. The switch uses the MAC address to identify which attached device outgoing packets are being sent from and where to deliver incoming packets.

So the MAC address identifies the physical device as opposed to the network layer (Layer 3) IP address, which can be assigned dynamically to a device and change over time.

When a device sends a packet to another device, it enters the switch and the switch reads its header to determine what to do with it. It matches the destination address or addresses and sends the packet out through the appropriate ports that leads to the destination devices.

To reduce the chance for collisions between network traffic going to and from a switch and a connected device at the same time, most switches offer full-duplex functionality in which packets coming from and going to a device have access to the full bandwidth of the switch connection. (Picture two people talking on a cell phone as opposed to a walkie-talkie).

While it's true that switches operate at Layer 2, they can also operate at Layer 3, which is necessary for them to support virtual LANs (VLAN), logical network segments that can span subnets. In order for traffic to get from one subnet to another it must pass between switches, and this is facilitated by routing capabilities built into the switches.

Switches vs. hubs
A hub can also connect several devices together for the purpose of sharing resources, and the collection of devices attached to a hub is known as a LAN segment.

A hub differs from a switch in that packets sent from one of the connected devices is broadcast to all of the devices that are connected to the hub. With a switch, packets are directed only to the port that leads to the device that packets are addressed to.

Switches typically connect LAN segments, so hubs attach to them. Switches filter out traffic destined for devices on the same LAN segment. Because of this intelligence, switches make more efficient use of their own processing resources as well as network bandwidth.

Switches vs. routers

Switches are sometimes confused with routers, which also offer forwarding and routing of network traffic, hence their name. But they do this with a different purpose and location.

Routers operate at Layer 3—the network layer—and are used to connect networks to other networks.

The difference between switches and routers is that devices connect locally LAN through switches, and networks are connected to other networks WAN through routers. If you think about the general path a packet might take to reach the Internet—for example: device > hub > switch > router > internet—that should help as well.

Of course, there are cases where switching functionality is built into a router hardware, and the router performs as the switch as well.

The easiest case here is to think of your home wireless router. It routes to a broadband connection through its WAN port, but it usually also has additional Ethernet ports that you can use to connect an Ethernet cable for a computer, television, printer or even a gaming console. While other devices on the network, such as other notebooks and phones, connect through the Wi-fi router, it still offers switching functions through the LAN. So the router, in effect, is also a switch. And you can even connect a separate switch to the router to provide both Internet and LAN access for additional devices.

Types of switches

Switches vary in size, depending on how many devices you need to connect in a specific area, as well as the type of network speed/bandwidth required for those devices. In a small office or home office, a four- or eight-port switch usually suffices, but for larger deployments you generally see switches up to 128 ports. The form factor of a smaller switch is an appliance that you can fit on a desktop, but switches are also rack-mountable for placement in a wiring closet or data center or server farm. Switches also vary in the network speed they offer, ranging from Fast Ethernet (10/100 Mbps), Gigabit Ethernet (10/100/1000 Mbps), 10 Gigabit (10/100/1000/10000 Mbps) and even 40/100 Gbps speeds. Which speed to choose depends on the throughput needed for the tasks being supported.

Switches also differ in their capabilities. Here are three types.

Unmanaged

Unmanaged switches are the most basic, offering fixed configuration. They are generally plug-and-play, which means they have few if any options for the user to choose from. They may have default settings for features such as quality of service, but they cannot be changed. The upside is that unmanaged switches are relatively inexpensive, but their lack of features make them unsuitable for most enterprise uses.

Managed

Managed switches offer more functionality and features for IT professionals and are the type most likely seen in business or enterprise settings. Managed switches have command-line interfaces (CLI) to configure them. They support simple network management protocol (SNMP) agents that provide information that can be used to troubleshoot network problems.

They can also support virtual LANs, quality of service settings and IP routing. The security is also better, protecting all types of traffic that they handle.

Because of their advanced features, managed switches cost much more than unmanaged switches.

Smart or intelligent switches

Smart or intelligent switches are managed switches that have some features beyond what an unmanaged switch offers, but fewer than a managed switch. So they are more sophisticated than unmanaged switches, but they are also less expensive than a fully manageable switch. They generally lack support for telnet access and have Web GUIs rather than CLIs. Other options, such as VLANs, may not have as many features as those supported by fully managed switches. But because they are less expensive, they may be a good fit for smaller networks with fewer financial resources and those with fewer feature needs.

Management features

The full list of features and functionalities of a network switch will vary depending on the switch manufacturer and any additional software provided, but in general a switch will offer professionals the ability to:

- Enable and disable specific ports on the switch.
- Configure settings for duplex (half or full), as well as bandwidth.
- Set quality of service (QoS) levels for a specific port.
- Enable MAC filtering and other access control features.
- Set up SNMP monitoring of devices, including the health of the link.
- Configure port mirroring, for monitoring network traffic.

Other uses

In larger networks, switches are often used as a way to offload traffic for analytic purposes. This can be important to security, where a switch can be placed in front of a WAN router, before the traffic goes to the LAN. It can facilitate intrusion detection, performance analytics, and firewalling. In many cases, port mirroring is used to create a mirror image of the data flowing through the switch before it is sent to an intrusion detection system or packet sniffer, for example.

At its most basic, however, it is the simple task for a network switch to quickly and efficiently deliver packets from computer A to computer B, whether the computers are located across the hallway or halfway around the world. Several other devices contribute to this delivery along the way, but the switch is an essential part of the networking architecture.

WAN Link Connection Options.

ISPs can use several WAN access connection options 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 shown in Figure 10.1 and described in the list that follows, an enterprise can get WAN access in two ways.

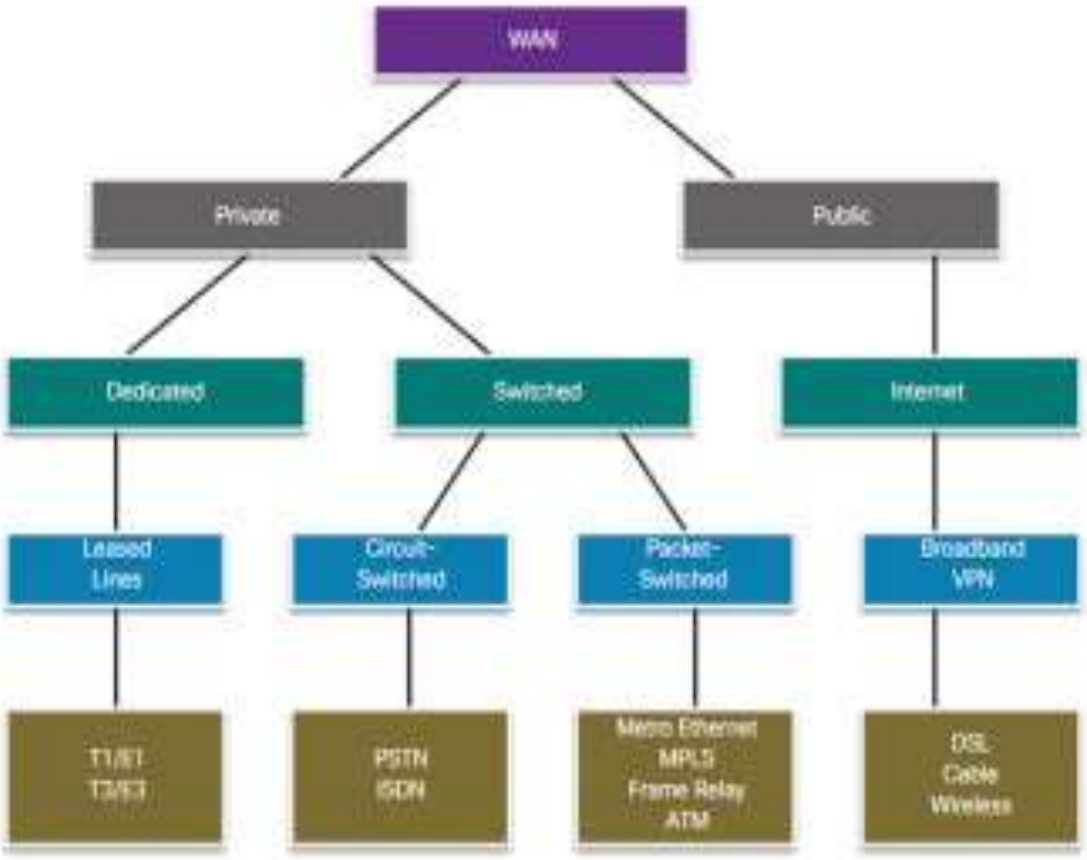

Fig 10.1 WAN Access Options

- *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 providers provide Internet access using broadband services such as DSL, cable, and satellite access. *Broadband connections* 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 Virtual Private Networks VPNs.

NOTE

Frame Relay systems are commonly being replaced by Ethernet WANs.

The topology in Figure 10.2 illustrates some of these WAN access technologies.

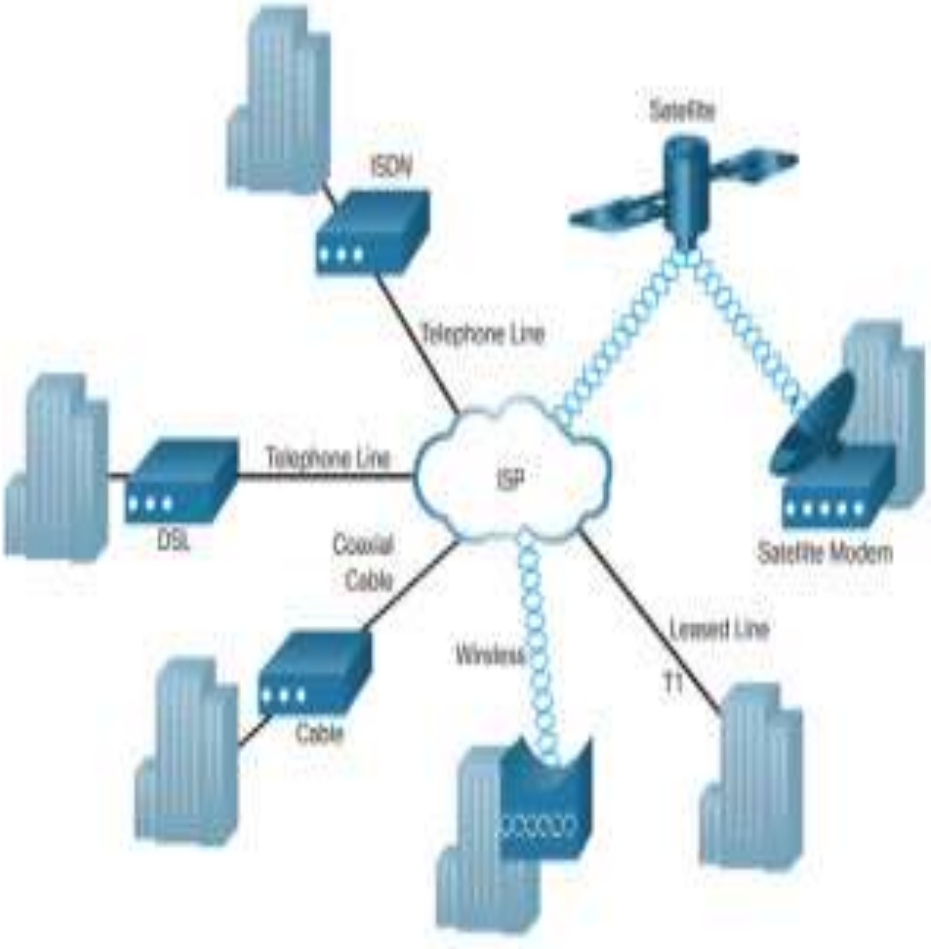

Fig 10.2 WAN Access Technologies

Service Provider Network Infrastructure.

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 LASER 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 10.3.

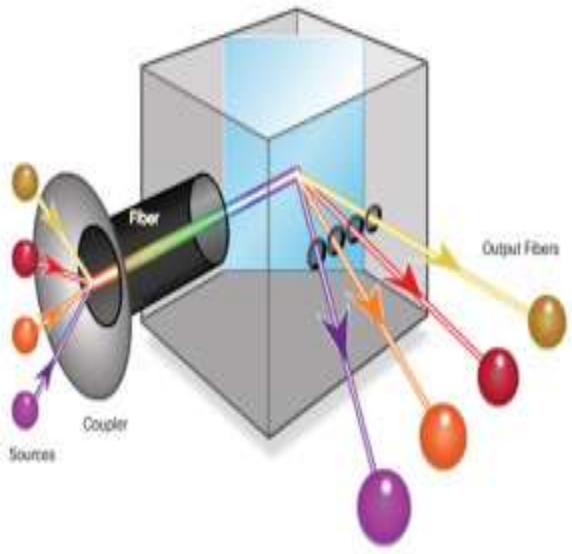

Fig 10.3 DWDM

DWDM enables long-range communication in several ways:

- DWDM enables bidirectional (for example, two-way) communications over one strand of fiber.
- It can *multiplex* more than 80 different channels of data (that is, wavelengths) onto a single fiber.
- Each channel is capable of carrying a 10 Gb/s multiplexed signal.
- It assigns incoming optical signals to specific wavelengths of light (that is, frequencies).
- It can amplify these wavelengths to boost the signal strength.
- It supports SONET and SDH standards.

DWDM circuits are used in all modern submarine communications cable systems and other long-haul circuits, as illustrated in Figure 10.4.

Fig 10.4 Service Provider Networks Use DWDM

Private WAN Infrastructures.

We compare private WAN technologies.

Leased Lines

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; for this reason, they 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 10.5. For instance, a T1 link supports 1.544 Mb/s, an E1 supports 2.048 Mb/s, a T3 supports 43.7 Mb/s, and an E3 connection supports 34.368 Mb/s. *Optical carrier (OC)* transmission rates are used to define the digital transmitting capacity of a fiber-optic network.

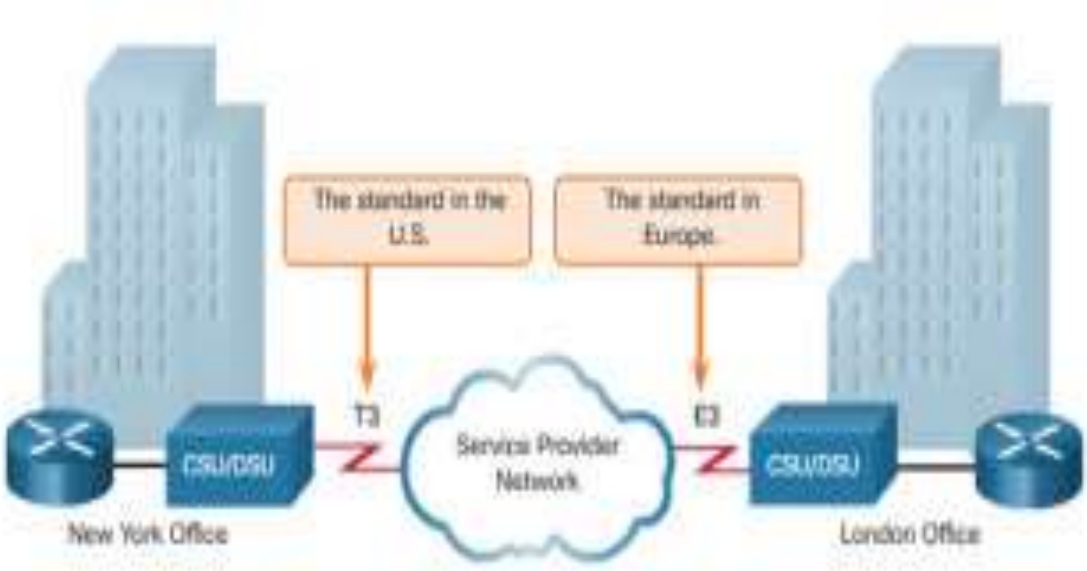

Fig 10.5 Sample Leased-Line Topology

Table 10-1 describes the advantages and disadvantages of using leased lines.

Table 10-1 Advantages/Disadvantages of Leased Lines

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

Advantages	Disadvantages
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.	**Limited flexibility:** WAN traffic is often variable, and leased lines have a fixed capacity, so 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.
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 Layer 2 protocol is usually HDLC or PPP.

Dialup

Dialup WAN access may be required when no other WAN technology is available. For example, a remote location could use modems and analog dialed telephone lines to provide low capacity and dedicated switched connections, as shown in 10.6. Dialup access is suitable when intermittent, low-volume data transfers are needed.

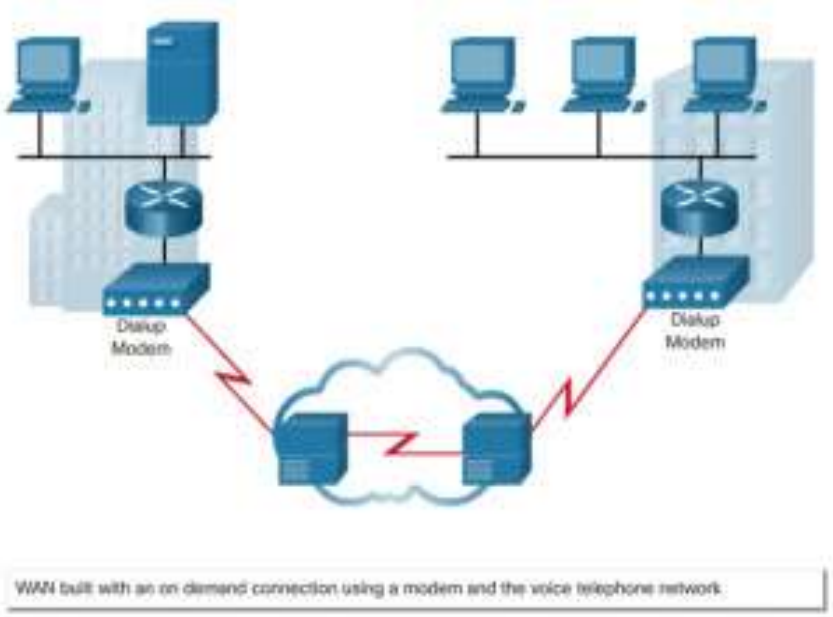

Fig 10.6 Sample Dialup Topology

Traditional telephony uses a copper cable, called 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 dialup 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 kb/s.

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 rates. These rates, often referred to as tariffs or toll charges, 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.

NOTE

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

ISDN

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 sub-channels in one communication channel. The signals appear to transfer simultaneously; but physically, the signals are taking turns on the channel.

Figure 10.7 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 10.7 Sample ISDN Topology

The two types of ISDN interfaces are as follows:

- **Basic Rate Interface (BRI):** ISDN BRI is intended for the home and small enterprise and provides two 64 kb/s bearer channels (B) for carrying voice and data and a 16 kb/s delta channel (D) for signaling, call setup, and other purposes. The BRI D channel is often underused because it has only two B channels to control (see 10.8).

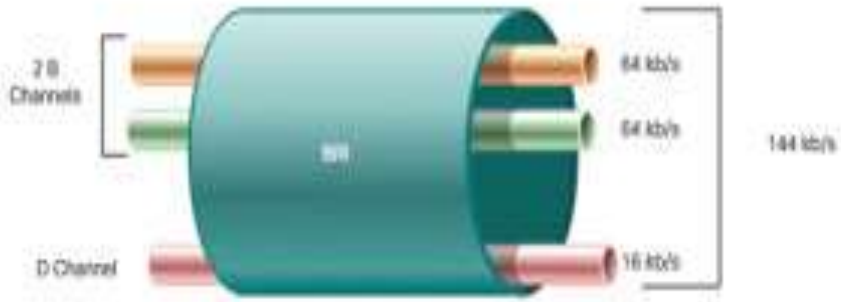

Figure 10.8 ISDN BRI

- *Primary Rate Interface (PRI)***:** ISDN is also available for larger installations. In North America, PRI delivers 23 B channels with 64 kb/s and one D channel with 64 kb/s for a total bit rate of up to 1.544 Mb/s. This includes some additional overhead for synchronization. In Europe, Australia, and other parts of the world, ISDN PRI provides 30 B channels and one D channel, for a total bit rate of up to 2.048 Mb/s, including synchronization overhead (see Figure 10.9).

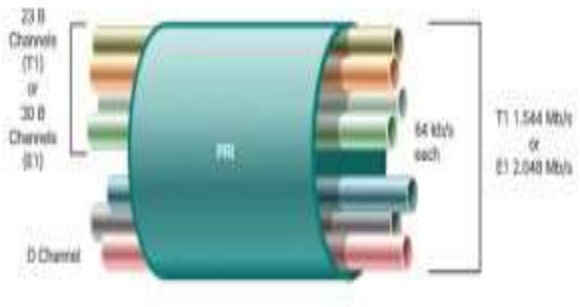

Figure 10.9 ISDN PRI

BRI has a call setup time that is less than a second, and the 64 kb/s B channel provides greater capacity than an analog modem link. In comparison, the call setup time of a dialup modem is approximately 30 or more seconds with a theoretical maximum of 56 kb/s. With ISDN, if greater capacity is required, a second B channel can be activated to provide a total of 128 kb/s. This permits several simultaneous voice conversations, a voice conversation and data transfer, or a video conference using one channel for voice and the other for video.

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 has declined in popularity as an Internet connection option with the introduction of high-speed DSL and other broadband services.

Frame Relay

Frame Relay is a simple Layer 2 *non-broadcast multi-access (NBMA)* WAN technology used to interconnect enterprise LANs. A single router interface can be used to connect to multiple sites using *permanent virtual circuits (PVCs)*. PVCs are used to carry both voice and data traffic between a source and destination, and support data rates up to 4 Mb/s, with some providers offering even higher rates.

An edge router requires only a single interface, even when multiple VCs are used. The 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 Figure 10.10, R1 will use DLCI 102 to reach R2 while R2 will use DLCI 201 to reach R1.

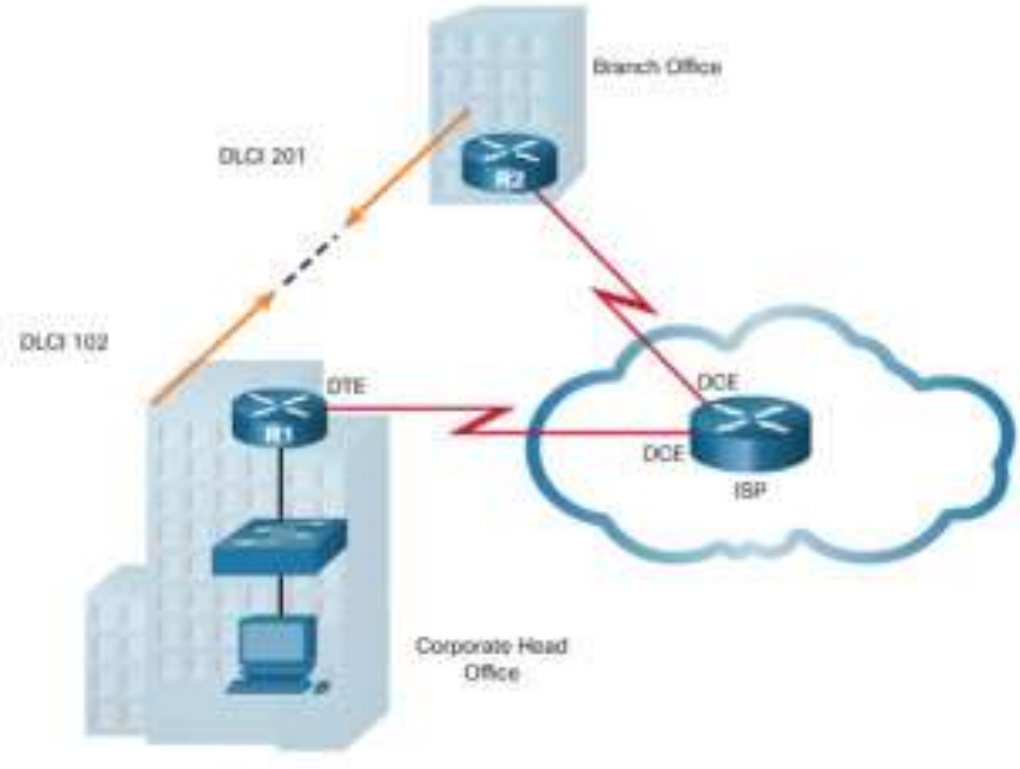

Figure 10.10 Sample Frame Relay Topology

ATM

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, as shown in Figure 10.11.

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.

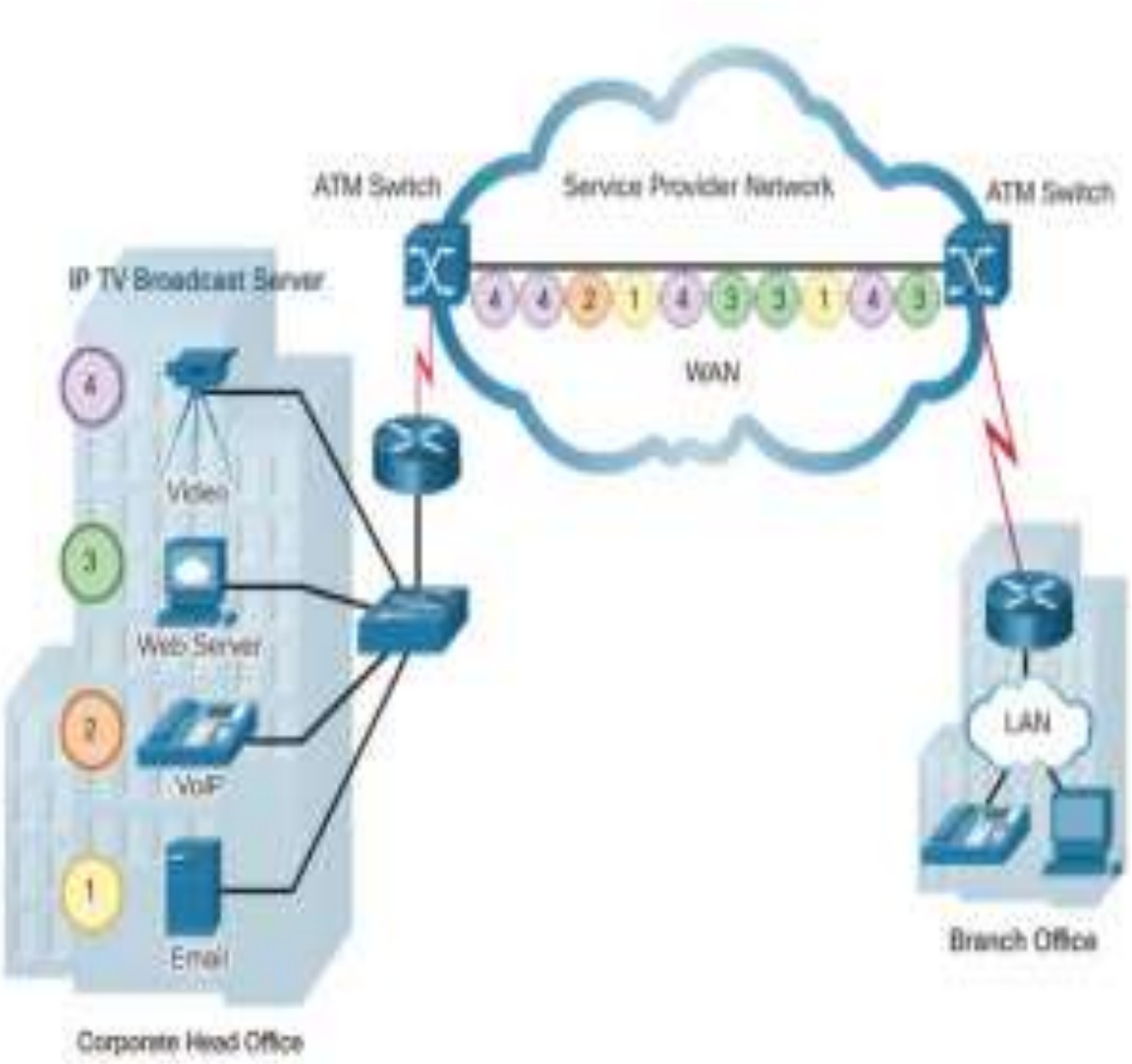

Figure 10.11 Sample ATM Topology

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

As with other shared technologies, ATM allows multiple VCs on a single leased-line connection to the network edge.

NOTE

ATM networks are now considered to be a legacy technology.

Ethernet WAN

Ethernet was originally developed to be a LAN access technology. Originally, Ethernet was not suitable as a WAN access technology because at that time, the maximum cable length was one 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 cable lengths up to 70 km.

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)*. A sample Ethernet WAN topology is shown in Figure 10.12.

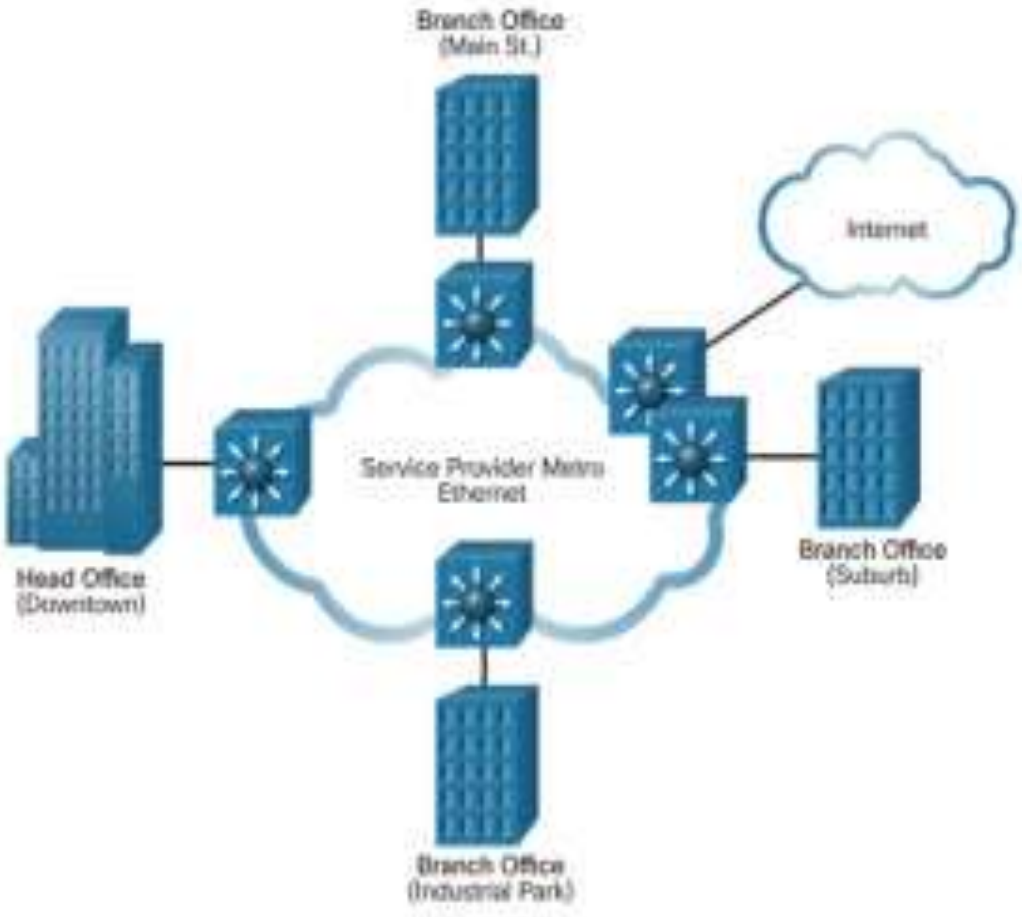

Figure 10.12 Sample Ethernet WAN Topology

An Ethernet WAN offers several benefits:

- **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

Multiprotocol Label Switching (MPLS) is a multiprotocol high-performance WAN technology that directs data from one router to the next. MPLS is 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 10.13 illustrates how MPLS is used. Notice that the different sites can connect to the MPLS cloud using different access technologies.

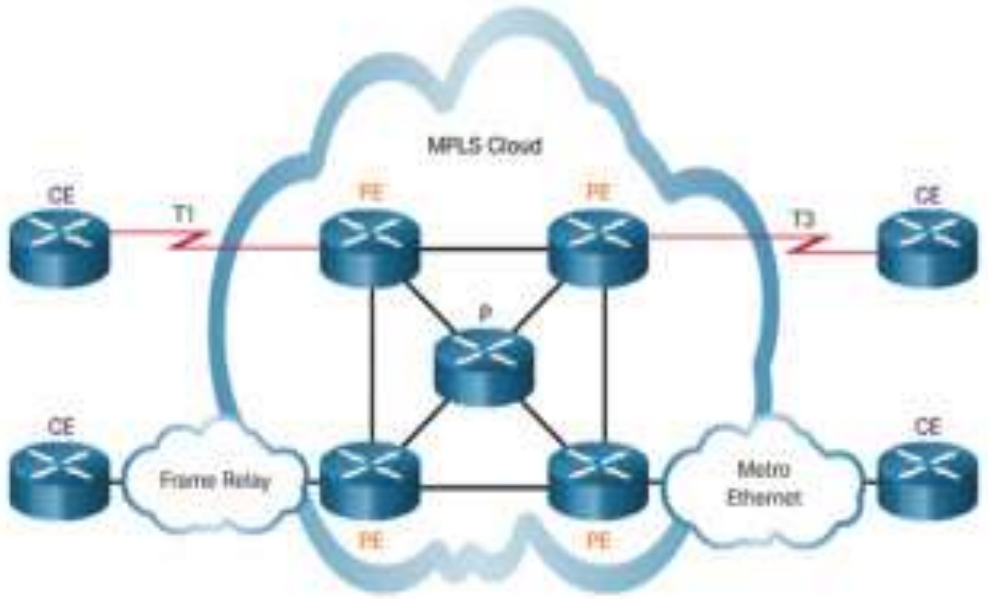

Figure 10.13 Sample MPLS Topology

In the Figure 10.13, CE refers to the customer edge; PE is the provider edge router, which adds and removes labels; and P is an internal provider router, which switches MPLS labeled packets.

VSAT

All private WAN technologies discussed so far used either copper or fiber-optic media. What if an organization needed connectivity in a remote location where no service providers 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. This satellite is in geosynchronous orbit in space. The signals must travel approximately 35,786 kilometers (22,236 miles) to the satellite and back.

The example in Figure 10.14 displays a VSAT dish on the roofs of the buildings communicating with a satellite thousands of kilometers away in space.

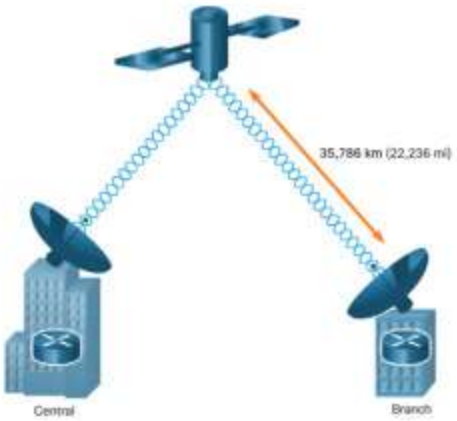

Figure 10.14 Sample VSAT Topology

Public WAN Infrastructure (1.2.3)

We compare public WAN technologies.

DSL

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 referred to as the *point of presence (POP)*. DSLAMs incorporate TDM technology to aggregate many subscriber lines into a single medium, generally a T3 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 10.15 displays a sample DSL WAN connection.

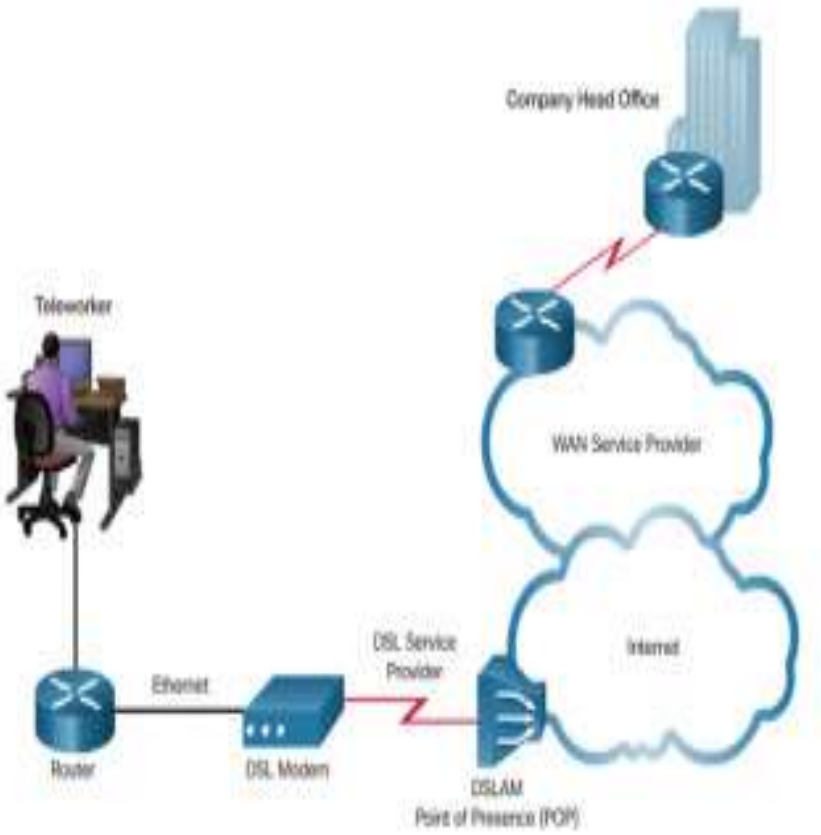

Figure 10.15 Sample DSL Topology

Cable

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

Cable modems (CMs) 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 drop below the expected rate.

The topology in Figure 10.16 displays a sample cable WAN connection.

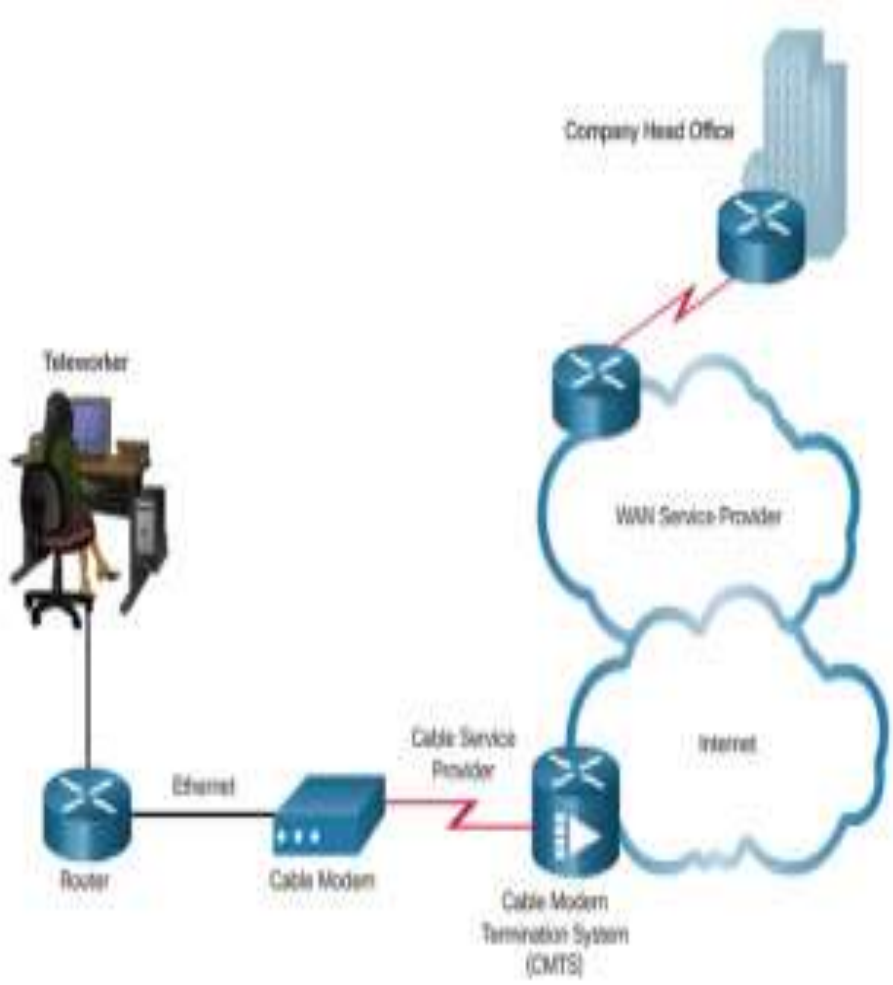

Figure 10.16 Sample Cable Topology

Source: https://e-tutes.com/lesson5/lan-switching-basics/

https://www.ciscopress.com/articles/article.asp?p=2832405&seqNum=5