

# CCNA 3 v7.0 Curriculum: Module 7 – WAN Concepts

---

 [itexamanswers.net/ccna-3-v7-0-curriculum-module-7-wan-concepts.html](https://itexamanswers.net/ccna-3-v7-0-curriculum-module-7-wan-concepts.html)

April 11, 2020

## Contents

---

## 7.0. Introduction

---

### 7.0.1. Why should I take this module?

---

Welcome to WAN Concepts!

As you know, local area networks are called LANs. The name implies that your LAN is local to you and your small home or office business. But what if your network is for a larger business, perhaps even a global enterprise? You cannot operate a large business with multiple sites without a wide area network, which is called a WAN. This module explains what WANs are and how they connect to the internet and also back to your LAN. Understanding the purpose and functions of WANs is foundational to your understanding of modern networks. So let's jump in to WAN Concepts!

### 7.0.2. What will I learn to do in this module?

---

**Module Title:** WAN Concepts

**Module Objective:** Explain how WAN access technologies can be used to satisfy business requirements.

Topic Title	Topic Objective
Purpose of WANs	Explain the purpose of a WAN.
WAN Operations	Explain how WANs operate.
Traditional WAN Connectivity	Compare traditional WAN connectivity options.
Modern WAN Connectivity	Compare modern WAN connectivity options.
Internet-Based Connectivity	Compare internet-based connectivity options.

## 7.1. Purpose of WANs

---

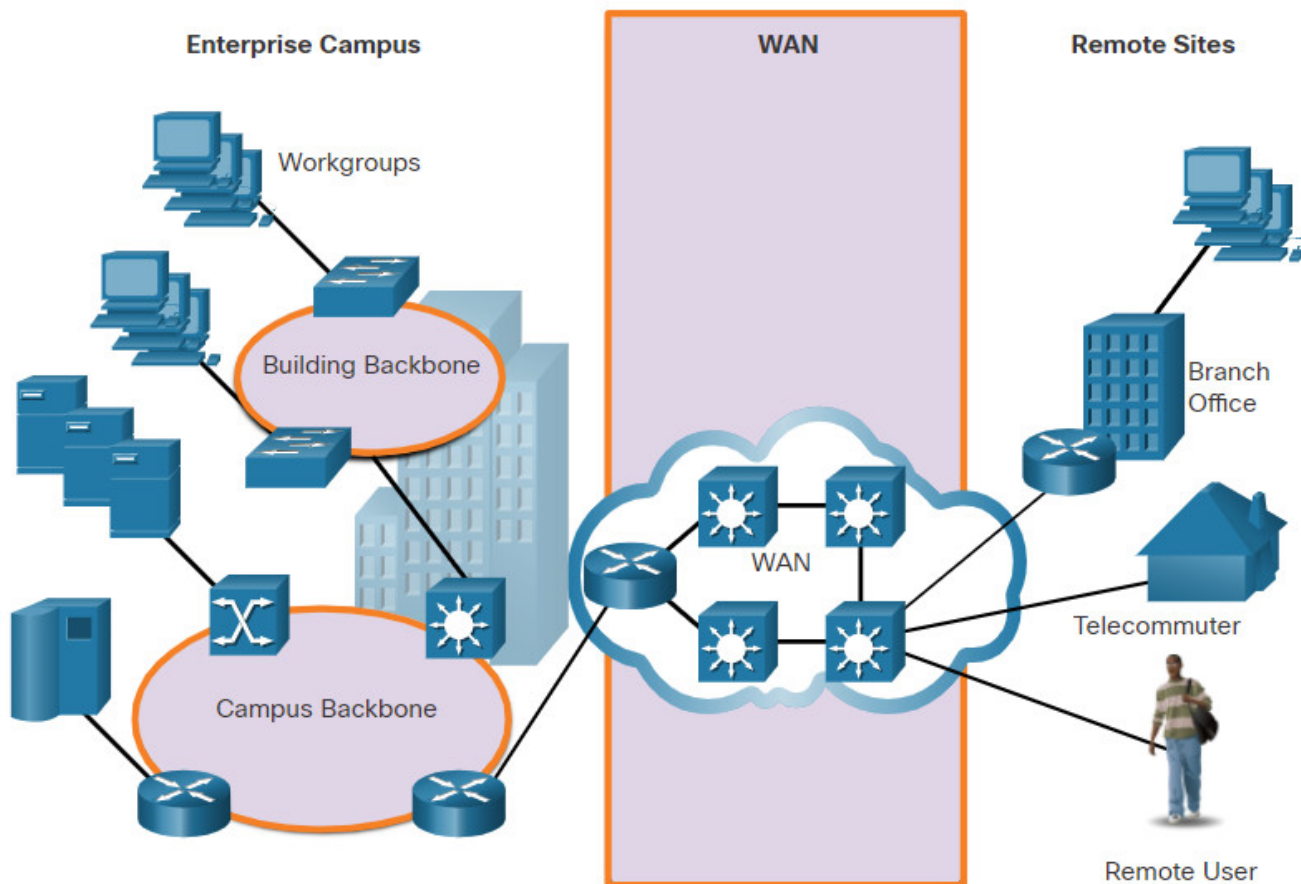
### 7.1.1. LANs and WANs

---

Whether at work or at home, we all use Local Area Networks (LANs). However, LANs are limited to a small geographical area.

A Wide Area Network (WAN) is required to connect beyond the boundary of the LAN. A WAN is a telecommunications network that spans over a relatively large geographical area. A WAN operates beyond the geographic scope of a LAN.

In the figure, WAN services are required to interconnect an enterprise campus network to remote LANs at branch sites, telecommuter sites, and remote users.



The table highlights differences between LANs and WANs.

### Local Area Networks (LANs)

LANs provide networking services within a small geographic area (i.e., home network, office network, building network, or campus network).

LANs are used to interconnect local computers, peripherals, and other devices.

### Wide Area Networks (WANs)

WANs provide networking services over large geographical areas (i.e., in and between cities, countries, and continents).

WANs are used to interconnect remote users, networks, and sites.

<b>Local Area Networks (LANs)</b>	<b>Wide Area Networks (WANs)</b>
A LAN is owned and managed by an organization or home user.	WANs are owned and managed by internet service, telephone, cable, and satellite providers.
Other than the network infrastructure costs, there is no fee to use a LAN.	WAN services are provided for a fee.
LANs provide high bandwidth speeds using wired Ethernet and Wi-Fi services.	WANs providers offer low to high bandwidth speeds, over long distances using complex physical networks.

### 7.1.2. Private and Public WANs

WANs may be built by a variety of different types of organizations, as follows:

- An organization that wants to connect users in different locations
- An ISP that wants to connect customers to the internet
- An ISP or telecommunications that wants to interconnect ISPs

A private WAN is a connection that is dedicated to a single customer. This provides for the following:

- Guaranteed service level
- Consistent bandwidth
- Security

A public WAN connection is typically provided by an ISP or telecommunications service provider using the internet. In this case, the service levels and bandwidth may vary, and the shared connections do not guarantee security.

### 7.1.3. WAN Topologies

Physical topologies describe the physical network infrastructure used by data when it is travelling from a source to a destination. The physical WAN topology used in WANs is complex and for the most part, unknown to users. Consider a user in New York establishing a video conference call with a user in Tokyo, Japan. Other than the user's internet connection in New York, it would not be feasible to identify the all of the actual physical connections that are needed to support the video call.

Instead, WAN topologies are described using a logical topology. Logical topologies describe the virtual connection between the source and destination. For example, the video conference call between the user in New York and Japan would be a logical point-to-point connection.

WANs are implemented using the following logical topology designs:

- Point-to-Point Topology
- Hub-and-Spoke Topology
- Dual-homed Topology
- Fully Meshed Topology
- Partially Meshed Topology

**Note:** Large networks usually deploy a combination of these topologies.

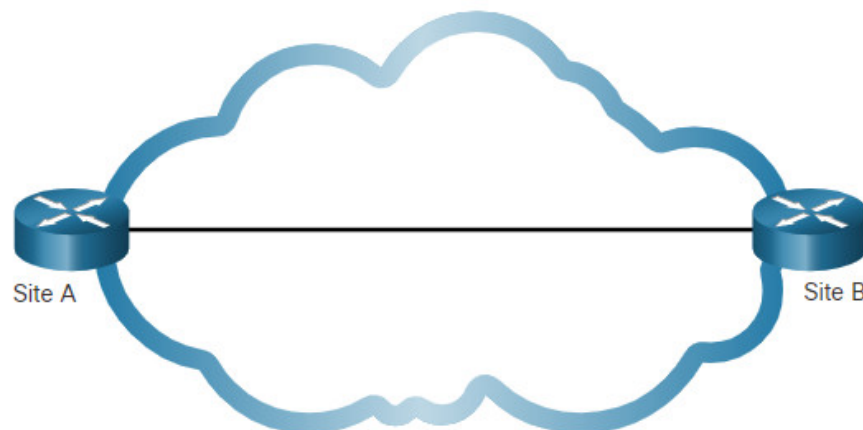
Click each button for an illustration and explanation of each WAN logical topology.

### Point-to-Point Topology

A point-to-point topology, as shown in the figure, employs a point-to-point circuit between two endpoints.

Point-to-point links often involve dedicated, leased-line connections from the corporate edge point to the provider networks. A point-to-point connection involves a Layer 2 transport service through the service provider network. Packets sent from one site are delivered to the other site and vice versa. A point-to-point connection is transparent to the customer network. It seems as if there is a direct physical link between two endpoints.

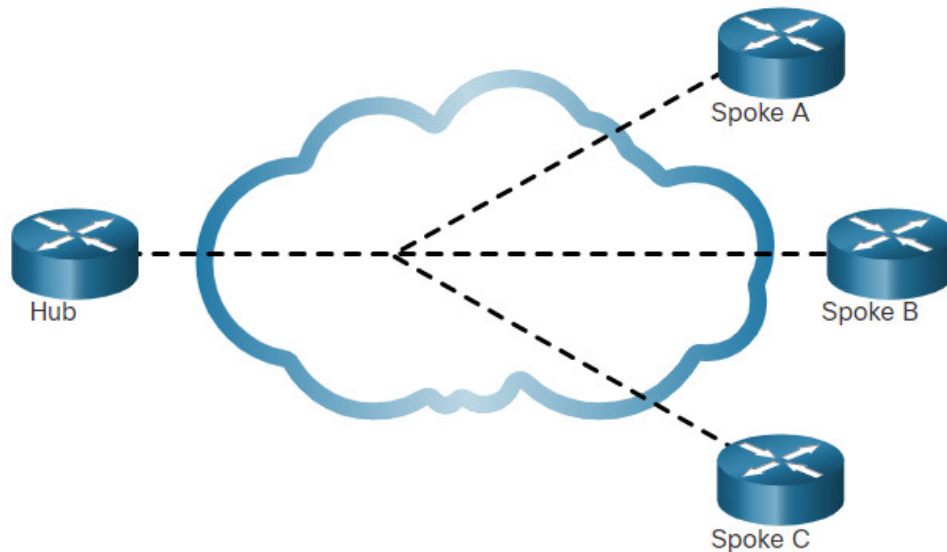
It can become expensive if many point-to-point connections are required.



### Hub-and-Spoke Topology

A hub-and-spoke topology enables a single interface on the hub router to be shared by all spoke circuits. Spoke routers can be interconnected through the hub router using virtual circuits and routed subinterfaces. The figure displays a sample hub-and-spoke topology consisting of three spoke routers connecting to a hub router across a WAN cloud.

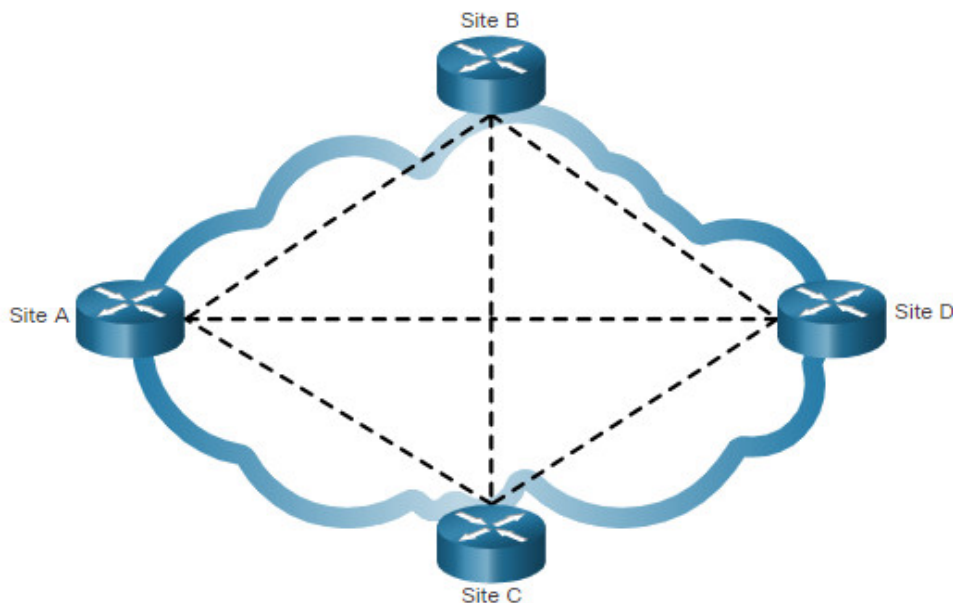
A hub-and-spoke topology is a single-homed topology. There is only one hub router and all communication must go through it. Therefore, spoke routers can only communicate with each other through the hub router. Consequently, the hub router represents a single point of failure. If it fails, inter-spoke communication also fails.



### Fully Meshed Topology

A fully meshed topology uses multiple virtual circuits to connect all sites, as shown in the figure.

This is the most fault-tolerant topology of the five shown. For instance, if site B lost connectivity to site A, it could send the data through either site C or site D.



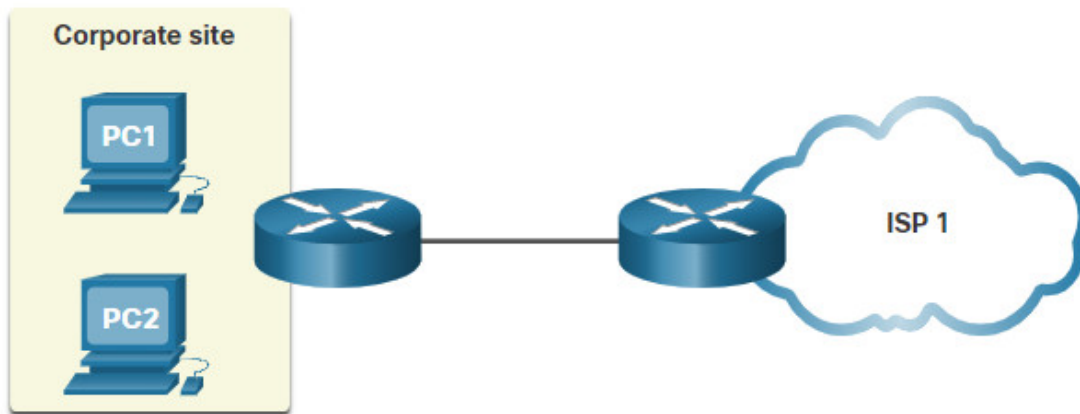
#### 7.1.4. Carrier Connections

Another aspect of WAN design is how an organization connects to the internet. An organization usually signs a service level agreement (SLA) with a service provider. The SLA outlines the expected services relating to the reliability and availability of the connection. The service provider may or may not be the actual carrier. A carrier owns and maintains the physical connection and equipment between the provider and the customer. Typically, an organization will choose either a single-carrier or dual-carrier WAN connection.

Click each button for an illustration and explanation of each carrier connection type.

### Single-Carrier WAN Connection

A single-carrier connection is when an organization connects to only one service provider, as shown in the figure. An SLA is negotiated between the organization and the service provider. The disadvantage of this design is the carrier connection and service provider are both single points of failure. Connectivity to the internet would be lost if the carrier link or the provider router failed.



### 7.1.5. Evolving Networks

---

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 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. They must also optimize their networks by using a variety of network design techniques and architectures.

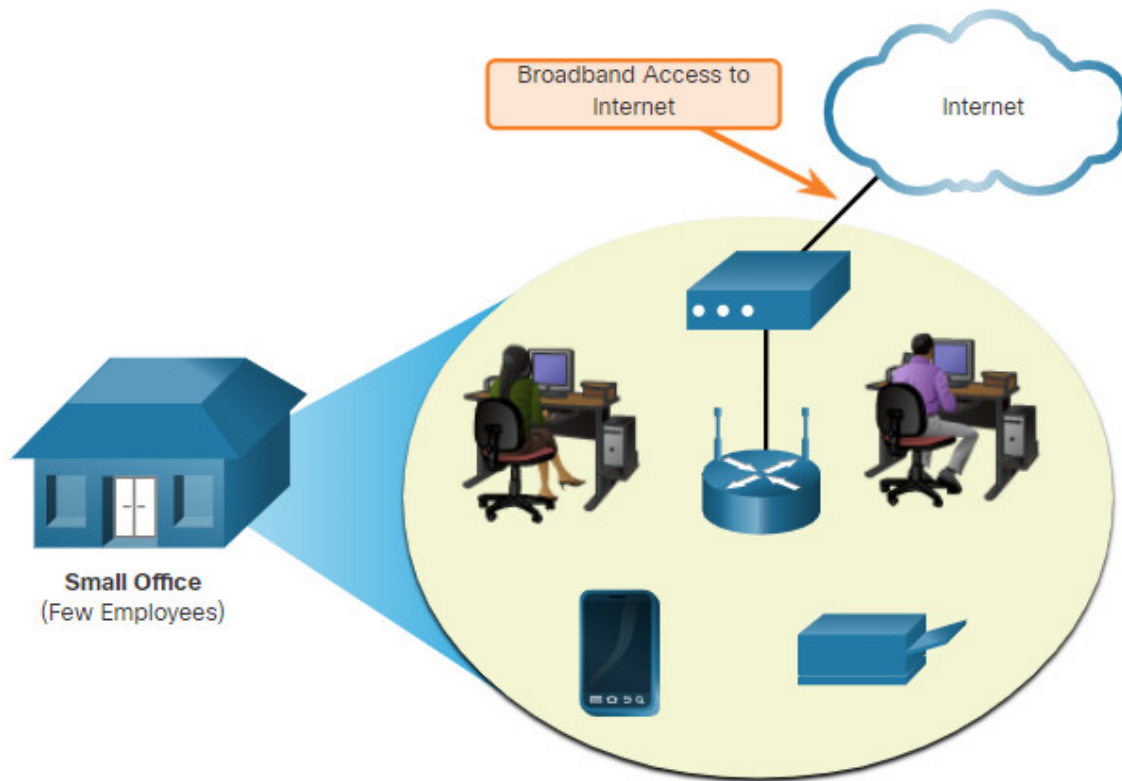
To illustrate differences between network size, we will use a fictitious company called SPAN Engineering as it grows from a small, local, business into a global enterprise. SPAN Engineering, an environmental consulting firm, has developed a special process for converting household waste into electricity and is developing a small pilot project for a municipal government in its local area.

Click each button for an illustration and description of the SPAN network as it evolves from a small network to a global enterprise.

#### Small Network

The company initially consisted of 15 employees working in a small office, as shown in the figure.

They used a single LAN that was connected to a wireless router for sharing data and peripherals. The connection to the internet is through a common broadband service called Digital Subscriber Line (DSL), which is supplied by their local telephone service provider. To support their IT requirements, they contracted services from the DSL provider.



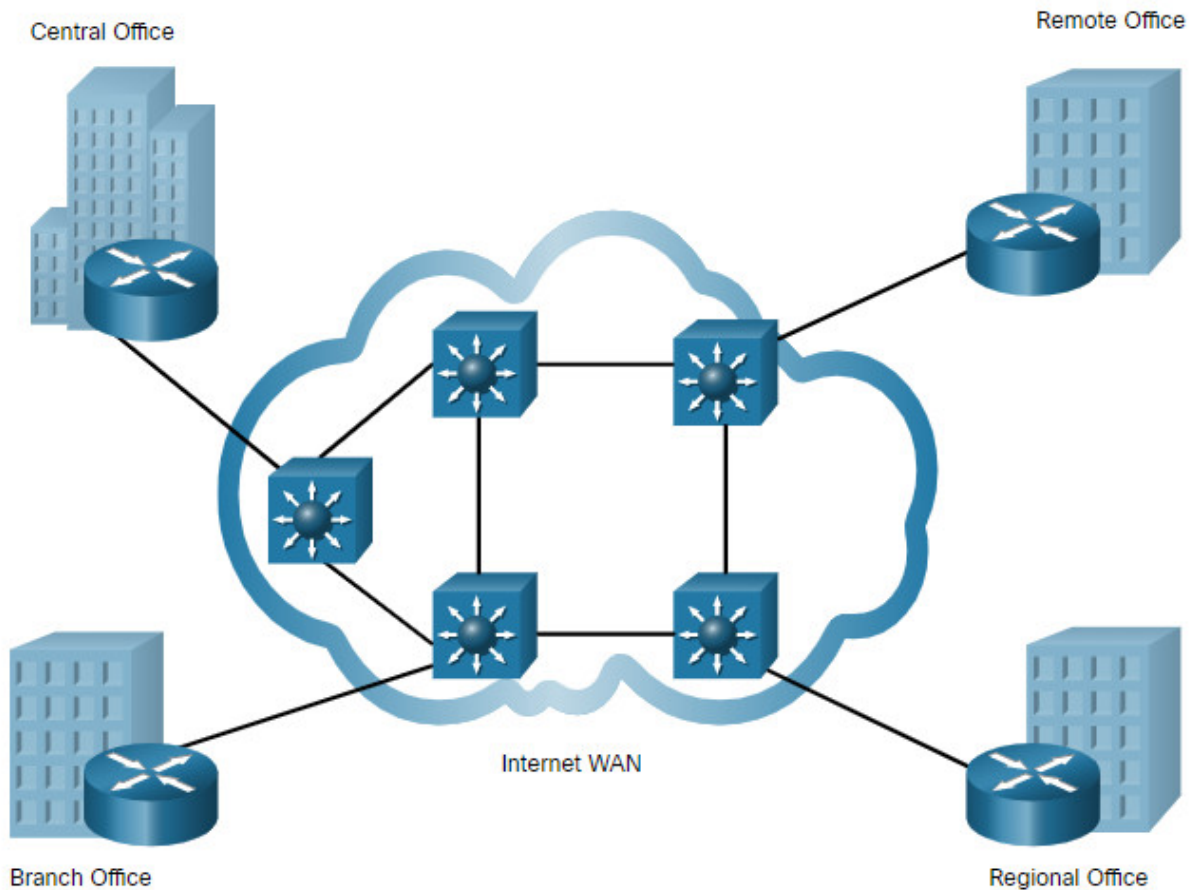
### Branch Network

A few years later, the company expanded and added a branch site in the city, and remote and regional sites in other cities, as shown in the figure.

The company now required a metropolitan area network (MAN) to interconnect sites within the city. A MAN is larger than a LAN, but smaller than a WAN.

To connect to the central office, branch offices in nearby cities used private dedicated lines through their local service provider. Offices in other cities and countries require the services of a WAN or may use internet services to connect distant locations. However, the internet introduces security and privacy issues that the IT team must address.





### **Distributed Network**

SPAN Engineering has now been in business for 20 years and has grown to thousands of employees distributed in offices worldwide, as shown in the figure.

To reduce network costs, SPAN encouraged teleworking and virtual teams using web-based applications, including web-conferencing, e-learning, and online collaboration tools 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.





## 7.2. WAN Operations

---

### 7.2.1. WAN Standards

---

Now that you understand how critical WANs are to large networks, this topic discusses how they work. The concept of a WAN has been around for many years. Consider that the telegraph system was the first large-scale WAN, followed by radio, telephone system, television, and now data networks. Many of the technologies and standards developed for these WANs were used as the basis for network WANs.

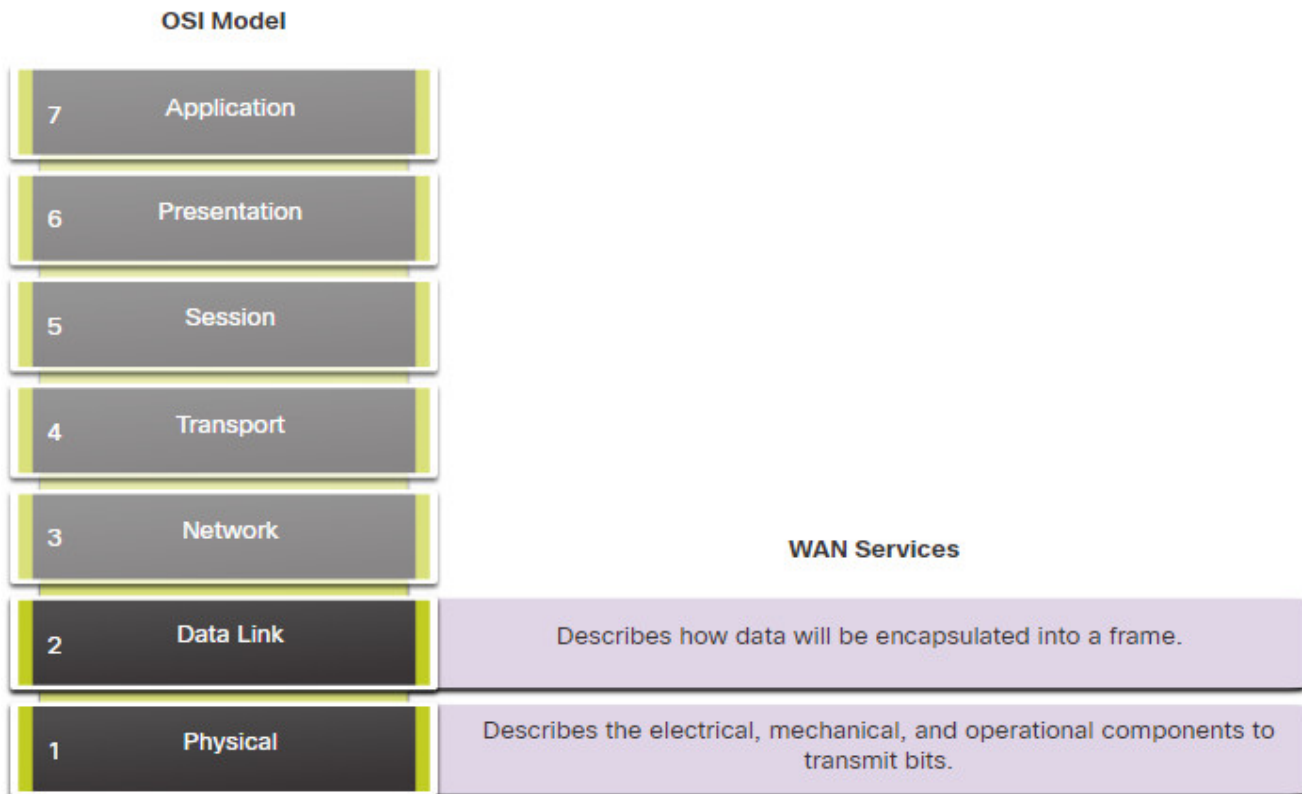
Modern WAN standards are defined and managed by a number of recognized authorities including the following:

- **TIA/EIA** – Telecommunications Industry Association and Electronic Industries Alliance
- **ISO** – International Organization for Standardization
- **IEEE** – Institute of Electrical and Electronics Engineers

### 7.2.2. WANs in the OSI Model

---

Most WAN standards focus on the physical layer (OSI Layer 1) and the data link layer (OSI Layer 2), as shown in the figure.



## Layer 1 Protocols

Layer 1 protocols describe the electrical, mechanical, and operational components needed to transmit bits over a WAN. For example, service providers commonly use high-bandwidth optical fiber media to span long distances (i.e., long haul) using the following Layer 1 optical fiber protocol standards:

- Synchronous Digital Hierarchy (SDH)
- Synchronous Optical Networking (SONET)
- Dense Wavelength Division Multiplexing (DWDM)

SDH and SONET essentially provide the same services and their transmission capacity can be increased by using DWDM technology.

## Layer 2 Protocols

Layer 2 protocols define how data will be encapsulated into a frame.

Several Layer 2 protocols have evolved over the years including the following:

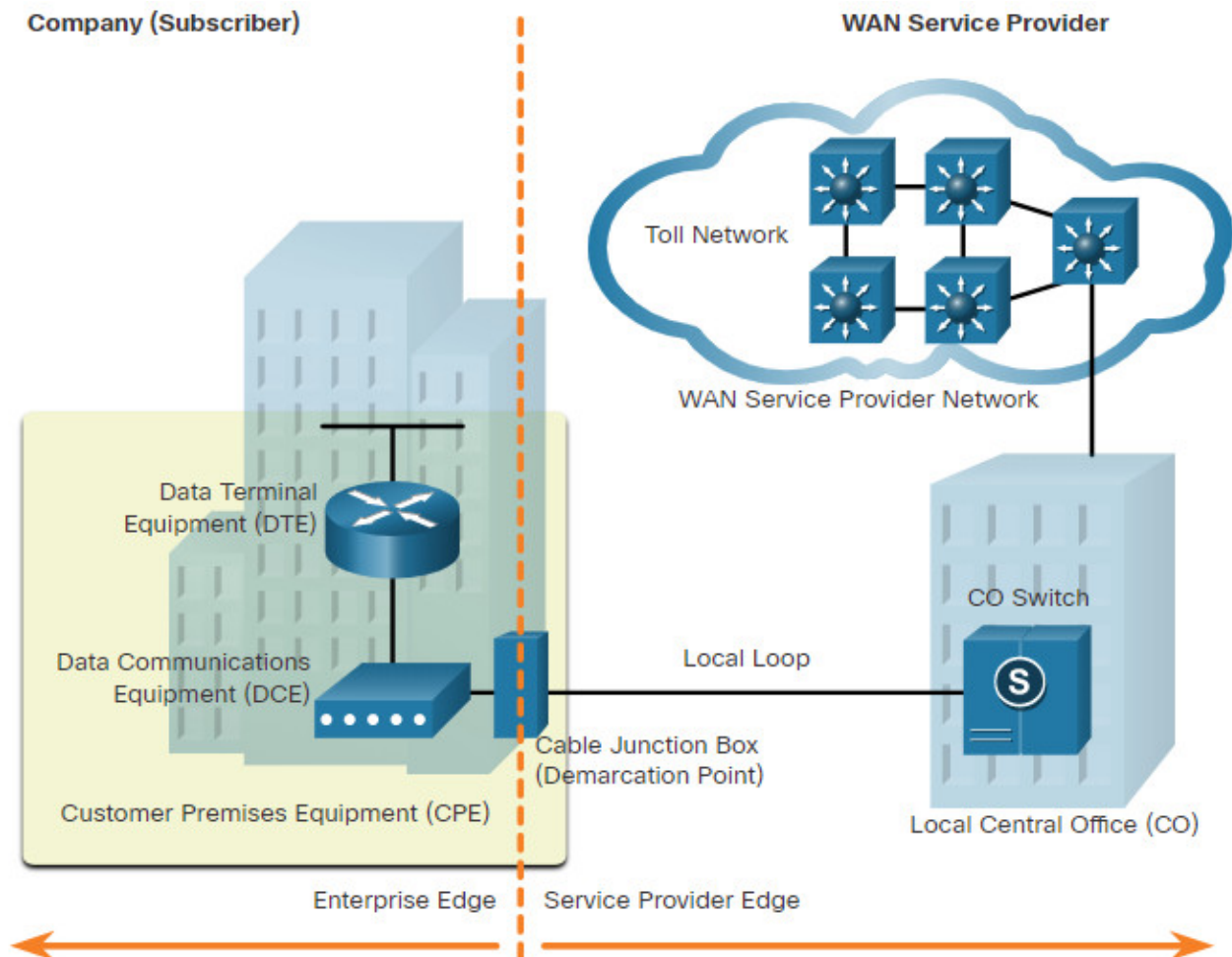
- Broadband (i.e., DSL and Cable)
- Wireless
- Ethernet WAN (Metro Ethernet)
- Multiprotocol Label Switching (MPLS)
- Point-to-Point Protocol (PPP) (less used)

- High-Level Data Link Control (HDLC) (less used)
- Frame Relay (legacy)
- Asynchronous Transfer Mode (ATM) (legacy)

### 7.2.3. Common WAN Terminology

The WAN physical layer describes the physical connections between the company network and the service provider network.

There are specific terms used to describe WAN connections between the subscriber (i.e., the company / client) and the WAN service provider, as shown in the figure.



Refer to the table for an explanation of the term shown in the figure, as well as some additional WAN-related terms.

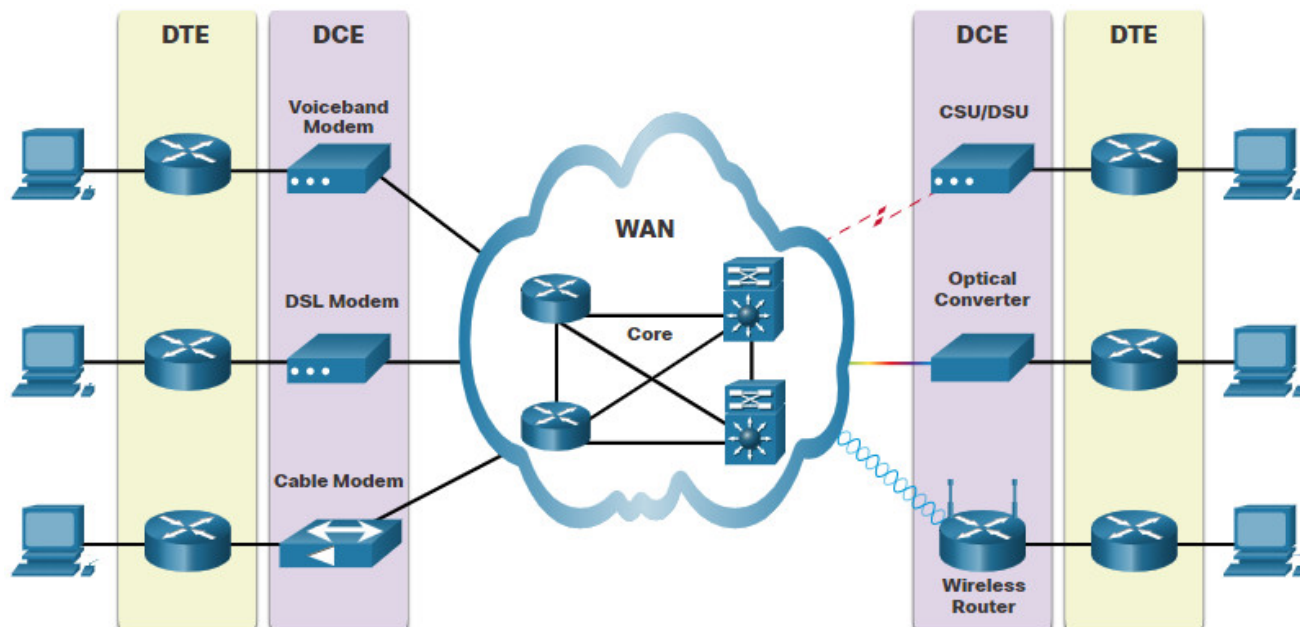
WAN Term	Description
----------	-------------

<b>WAN Term</b>	<b>Description</b>
<b>Data Terminal Equipment (DTE)</b>	<ul style="list-style-type: none"> <li>• This is the device that connects the subscriber LANs to the WAN communication device (i.e., DCE).</li> <li>• Inside hosts send their traffic to the DTE device.</li> <li>• The DTE connects to the local loop through the DCE.</li> <li>• The DTE device is usually a router but could be a host or server.</li> </ul>
<b>Data Communications Equipment (DCE)</b>	<ul style="list-style-type: none"> <li>• Also called data circuit-terminating equipment, this is the device used to communicate with the provider.</li> <li>• The DCE primarily provides an interface to connect subscribers to a communication link on the WAN cloud.</li> </ul>
<b>Customer Premises Equipment (CPE)</b>	<ul style="list-style-type: none"> <li>• This is the DTE and DCE devices (i.e., router, modem, optical converter) located on the enterprise edge.</li> <li>• The subscriber either owns the CPE or leases the CPE from the service provider.</li> </ul>
<b>Point-of-Presence (POP)</b>	This is the point where the subscriber connects to the service provider network.
<b>Demarcation Point</b>	<ul style="list-style-type: none"> <li>• This is a physical location in a building or complex that officially separates the CPE from service provider equipment.</li> <li>• The demarcation point is typically a cabling junction box, located on the customer premises, that connects the CPE wiring to the local loop.</li> <li>• It identifies the location where the network operation responsibility changes from the subscriber to the service provider.</li> <li>• When problems arise, it is necessary to determine whether the user or the service provider is responsible for troubleshooting or repair.</li> </ul>
<b>Local Loop (or last mile)</b>	This is the actual copper or fiber cable that connects the CPE to the CO of the service provider.
<b>Central Office (CO)</b>	This is the local service provider facility or building that connects the CPE to the provider network.
<b>Toll network</b>	This includes backhaul, long-haul, all-digital, fiber-optic communications lines, switches, routers, and other equipment inside the WAN provider network.

WAN Term	Description
<b>Backhaul network</b>	<ul style="list-style-type: none"> <li>• (Not shown) Backhaul networks connect multiple access nodes of the service provider network.</li> <li>• Backhaul networks can span over municipalities, countries and regions.</li> <li>• Backhaul networks are also connected to internet service providers and to the backbone network.</li> </ul>
<b>Backbone network</b>	<ul style="list-style-type: none"> <li>• (Not shown) These are large, high-capacity networks used to interconnect service provider networks and to create a redundant network.</li> <li>• Other service providers can connect to the backbone directly or through another service provider.</li> <li>• Backbone network service providers are also called Tier-1 providers.</li> </ul>

#### 7.2.4. WAN Devices

There are many types of devices that are specific to WAN environments. However, the end-to-end data path over a WAN is usually from source DTE to the DCE, then to the WAN cloud, then to the DCE to and finally to the destination DTE, as shown in the figure.



Refer to table for an explanation of the WAN devices shown in the figure.

WAN Device	Description
------------	-------------

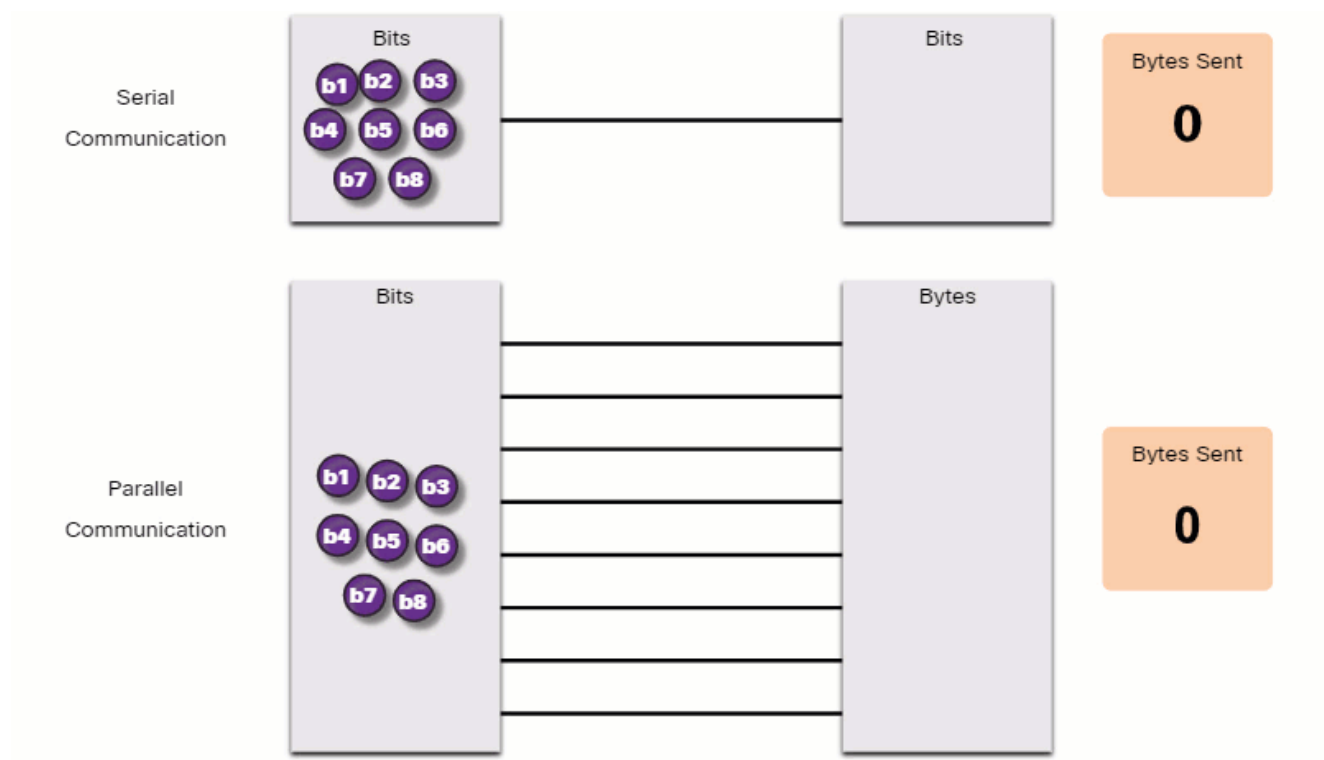
<b>WAN Device</b>	<b>Description</b>
<b>Voiceband Modem</b>	<ul style="list-style-type: none"> <li>• Also known as dial-up modem.</li> <li>• Legacy device that converted (i.e., modulated) the digital signals produced by a computer into analog voice frequencies.</li> <li>• Uses telephone lines to transmit data.</li> </ul>
<b>DSL Modem and Cable Modem</b>	<ul style="list-style-type: none"> <li>• Collectively known as broadband modems, these high-speed digital modems connect to the DTE router using Ethernet.</li> <li>• DSL modems connect to the WAN using telephone lines.</li> <li>• Cable modems connect to the WAN using coaxial lines.</li> <li>• Both operate in a similar manner to the voiceband modem but use higher broadband frequencies and transmission speeds.</li> </ul>
<b>CSU/DSU</b>	<ul style="list-style-type: none"> <li>• Digital-leased lines require a CSU and a DSU.</li> <li>• It connects a digital device to a digital line.</li> <li>• A CSU/DSU can be a separate device like a modem or it can be an interface on a router.</li> <li>• The CSU provides termination for the digital signal and ensures connection integrity through error correction and line monitoring.</li> <li>• The DSU converts the line frames into frames that the LAN can interpret and vice versa.</li> </ul>
<b>Optical Converter</b>	<ul style="list-style-type: none"> <li>• Also known as an optical fiber converter.</li> <li>• These devices connect fiber-optic media to copper media and convert optical signals to electronic pulses.</li> </ul>
<b>Wireless Router or Access Point</b>	<ul style="list-style-type: none"> <li>• Devices are used to wirelessly connect to a WAN provider.</li> <li>• Routers could also use cellular wireless connectivity.</li> </ul>
<b>WAN Core devices</b>	<ul style="list-style-type: none"> <li>• The WAN backbone consists of multiple high-speed routers and Layer 3 switches.</li> <li>• A router or multilayer switch must be able to support multiple telecommunications interfaces of the highest speed used in the WAN core.</li> <li>• It must also be able to forward IP packets at full speed on all those interfaces.</li> <li>• The router or multilayer switch must also support the routing protocols being used in the core.</li> </ul>

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

### 7.2.5. Serial Communication

Almost all network communications occur using a serial communication delivery. Serial communication transmits bits sequentially over a single channel. In contrast, parallel communications simultaneously transmit several bits using multiple wires.

Click Play to see an illustration of the difference between serial and parallel connections.



Although a parallel connection theoretically transfers data eight times faster than a serial connection, it is prone to synchronization problems. As the cable length increases, the synchronization timing between multiple channels becomes more sensitive to distance. For this reason, parallel communication is limited to very short distances only (e.g., copper media is limited to less than 8 meters (i.e., 26 feet).

Therefore, parallel communication is not a viable WAN communication method because of its length restriction. It is however a viable solution in data centers where distances between servers and switches are relatively short.

For instance, the Cisco Nexus switches in data centers support parallel optics solutions to transfer more data signals and achieve higher speeds (i.e., 40 Gbps and 100 Gbps).

### 7.2.6. Circuit-Switched Communication

Network communication can be implemented using circuit-switched communication. A circuit-switched network establishes a dedicated circuit (or channel) between endpoints before the users can communicate.



Specifically, circuit switching dynamically establishes a dedicated virtual connection through the service provider network before voice or data communication can start.

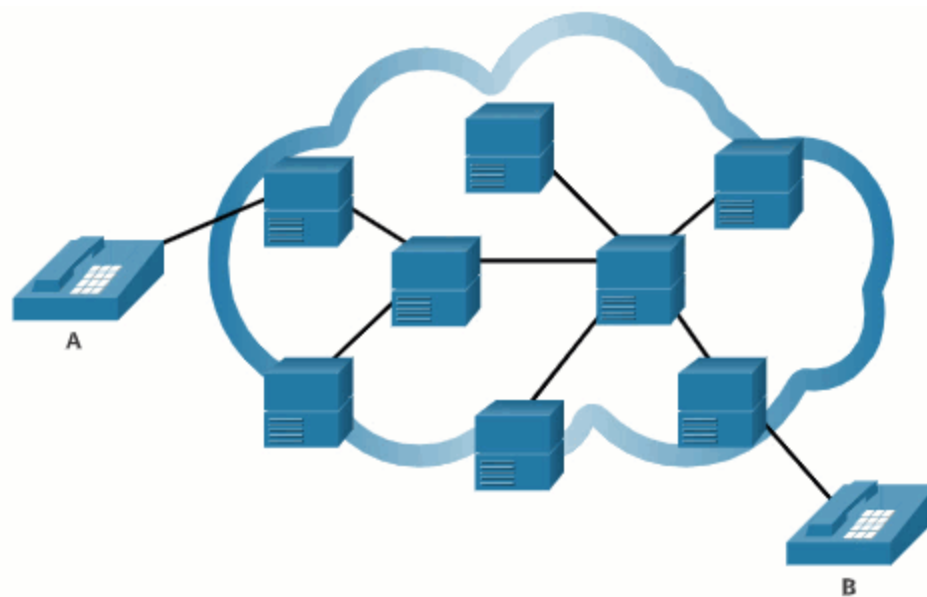
For example, when a user makes a telephone call using a landline, the number called is used by the provider equipment to create a dedicated circuit from the caller to the called party.

**Note:** A landline describes a telephone situated in a fixed location that is connected to the provider using copper or fiber-optic media.

During transmission over a circuit-switched network, all communication uses the same path. The entire fixed capacity allocated to the circuit is available for the duration of the connection, regardless of whether there is information to transmit or not. This can lead to inefficiencies in circuit usage. For this reason, circuit switching is generally not suited for data communication.

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

Click Play in the figure to see how circuit switching works.



Dialing sets up a physical circuit through the system.

### 7.2.7. Packet-Switched Communications

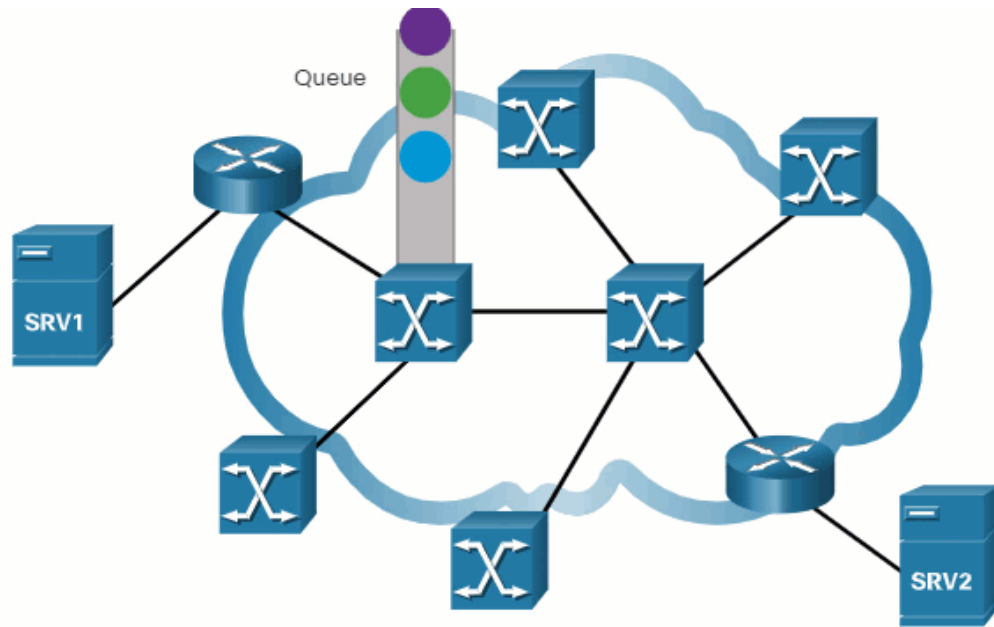
---

Network communication is most commonly implemented using packet-switched communication. In contrast to circuit-switching, packet-switching segments traffic data into packets that are routed over a shared network. Packet-switched networks do not require a circuit to be established, and they allow many pairs of nodes to communicate over the same channel.

Packet switching is much less expensive and more flexible than circuit switching. Although susceptible to delays (latency) and variability of delay (jitter), modern technology allows satisfactory transport of voice and video communications on these networks.

Common types of packet-switched WAN technologies are Ethernet WAN (Metro Ethernet), Multiprotocol Label Switching (MPLS), as well as legacy Frame Relay and legacy Asynchronous Transfer Mode (ATM).

Click Play in the figure to see a packet-switching example.



Labeled data is passed from switch to switch. It may have to wait its turn on a link.

### 7.2.8. SDH, SONET, and DWDM

Service provider networks use fiber-optic infrastructures to transport user data between destinations. Fiber-optic cable is far superior to copper cable for long distance transmissions due to its much lower attenuation and interference.

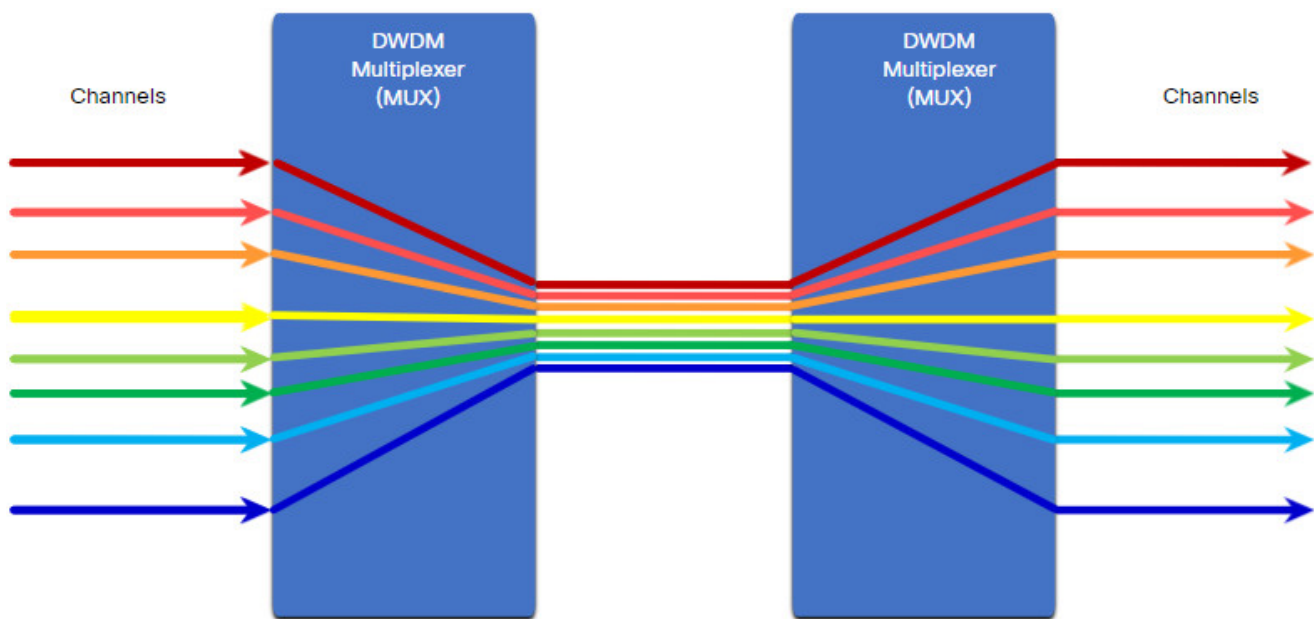
There are two optical fiber OSI layer 1 standards available to service providers:

- **SDH** – Synchronous Digital Hierarchy (SDH) is a global standard for transporting data over fiber-optic cable.
- **SONET** – Synchronous Optical Networking (SONET) is the North American standard that provides the same services as SDH.

Both standards are essentially the same and therefore, they are often listed as SONET/SDH.

SDH/SONET define how to transfer multiple data, voice, and video communications over optical fiber using lasers or light-emitting diodes (LEDs) over great distances. Both standards are used on the ring network topology that contains the redundant fiber paths that allow traffic to flow in both directions.

Dense Wavelength Division Multiplexing (DWDM) is a newer technology that increases the data-carrying capacity of SDH and SONET by simultaneously sending multiple streams of data (multiplexing) using different wavelengths of light, as shown in the figure.



DWDM has the following features:

- It supports SONET and SDH standards.
- It can multiplex more than 80 different channels of data (i.e., wavelengths) onto a single fiber.
- Each channel is capable of carrying a 10 Gbps multiplexed signal.
- It assigns incoming optical signals to specific wavelengths of light (i.e., frequencies).

**Note:** DWDM circuits are used in long-haul systems and modern submarine communications cable systems.

## 7.3. Traditional WAN Connectivity

---

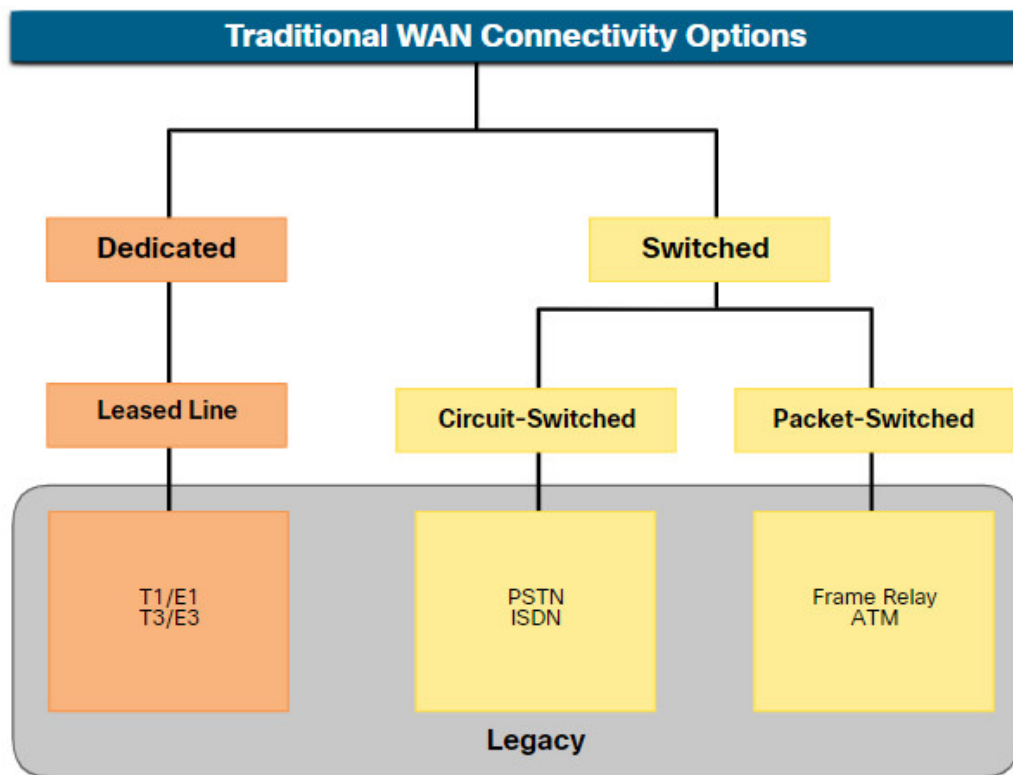
### 7.3.1. Traditional WAN Connectivity Options

---

To understand the WANs of today, it helps to know where they started. This topic discusses WAN connectivity options from the beginning. When LANs appeared in the 1980s, organizations began to see the need to interconnect with other locations. To do so, they

needed their networks to connect to the local loop of a service provider. This was accomplished by using dedicated lines, or by using switched services from a service provider.

The figure summarizes the traditional WAN connectivity options.



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

### 7.3.2. Common WAN Terminology

When permanent dedicated connections were required, a point-to-point link using copper media was used to provide a pre-established WAN communications path from the customer premises to the provider network. Point-to-point lines could be leased from a service provider and were called “leased lines”. The term refers to the fact that the organization pays a monthly lease fee to a service provider to use the line.

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.

Leased lines are available in different fixed capacities and are generally priced based on the bandwidth required and the distance between the two connected points.

There are two systems used to define the digital capacity of a copper media serial link:

- **T-carrier** – Used in North America, T-carrier provides T1 links supporting bandwidth up to 1.544 Mbps and T3 links supporting bandwidth up to 43.7 Mbps.
- **E-carrier** – Used in Europe, E-carrier provides E1 links supporting bandwidth up to 2.048 Mbps and E3 links supporting bandwidth up to 34.368 Mbps.

**Note:** The copper cable physical infrastructure has largely been replaced by optical fiber network. Transmission rates in optical fiber network are given in terms of Optical Carrier (OC) transmission rates, which define the digital transmitting capacity of a fiber-optic network.

The table summarizes the advantages and disadvantages of leased lines.

### Advantages

Simplicity	Point-to-point communication links require minimal expertise to install and maintain.
Quality	Point-to-point communication links usually offer high quality service, 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.

### Disadvantages

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.

### 7.3.3. Circuit-Switched Options

Circuit-switched connections are provided by Public Service Telephone Network (PSTN) carriers. The local loop connecting the CPE to the CO is copper media. There are two traditional circuit-switched options.

#### Public Service Telephone Network (PSTN)

Dialup WAN access uses the PSTN as its WAN connection. Traditional local loops can transport binary computer data through the voice telephone network using a voiceband modem. The modem modulates the digital data into an analog signal at the source and demodulates the analog signal to digital 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.

Dialup access is considered a legacy WAN technology. However, it may still be a viable solution when no other WAN technology is available.

### **Integrated Services Digital Network (ISDN)**

ISDN is a circuit-switching technology that enables the PSTN local loop to carry digital signals. This provided higher capacity switched connections than dialup access. ISDN provides for data rates from 45 Kbps to 2.048 Mbps.

ISDN has declined greatly in popularity due to high-speed DSL and other broadband services. ISDN is considered a legacy technology with most major providers discontinuing this service.

### **7.3.4. Packet-Switched Options**

---

Packet switching segments data into packets that are routed over a shared network. Circuit-switched networks require a dedicated circuit to be established. In contrast, packet-switching networks allow many pairs of nodes to communicate over the same channel.

There are two traditional (legacy) packet-switched connectivity options.

#### **Frame Relay**

Frame Relay is a simple Layer 2 non-broadcast multi-access (NBMA) WAN technology that is used to interconnect enterprise LANs. A single router interface can be used to connect to multiple sites using different 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.

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.

Frame Relay networks have been largely replaced by faster Metro Ethernet and internet-based solutions.

#### **Asynchronous Transfer Mode (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.

The 53-byte ATM cell is less efficient than the bigger frames and packets of Frame Relay. Furthermore, the ATM cell has at least five 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 networks have been largely replaced by faster Metro Ethernet and internet-based solutions.

## 7.4. Modern WAN Connectivity

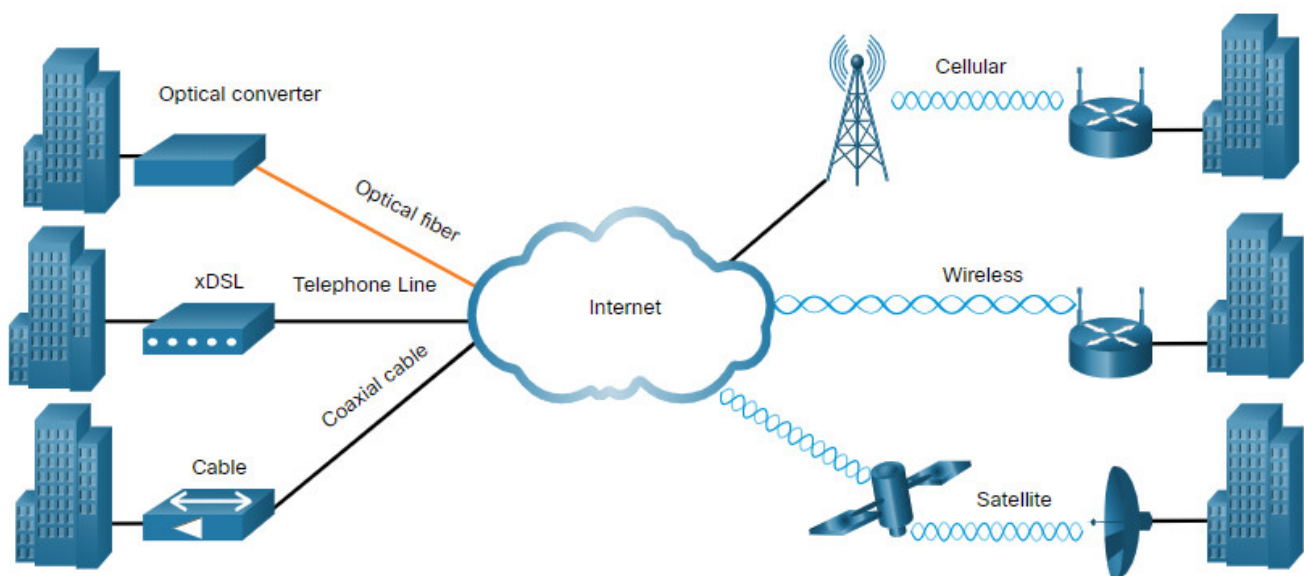
---

### 7.4.1. Modern WANs

---

Modern WANS have more connectivity options that traditional WANs. Enterprises now require faster and more flexible WAN connectivity options. Traditional WAN connectivity options have rapidly declined in use because they are either no longer available, too expensive, or have limited bandwidth.

The figure displays the local loop connections most likely encountered today.

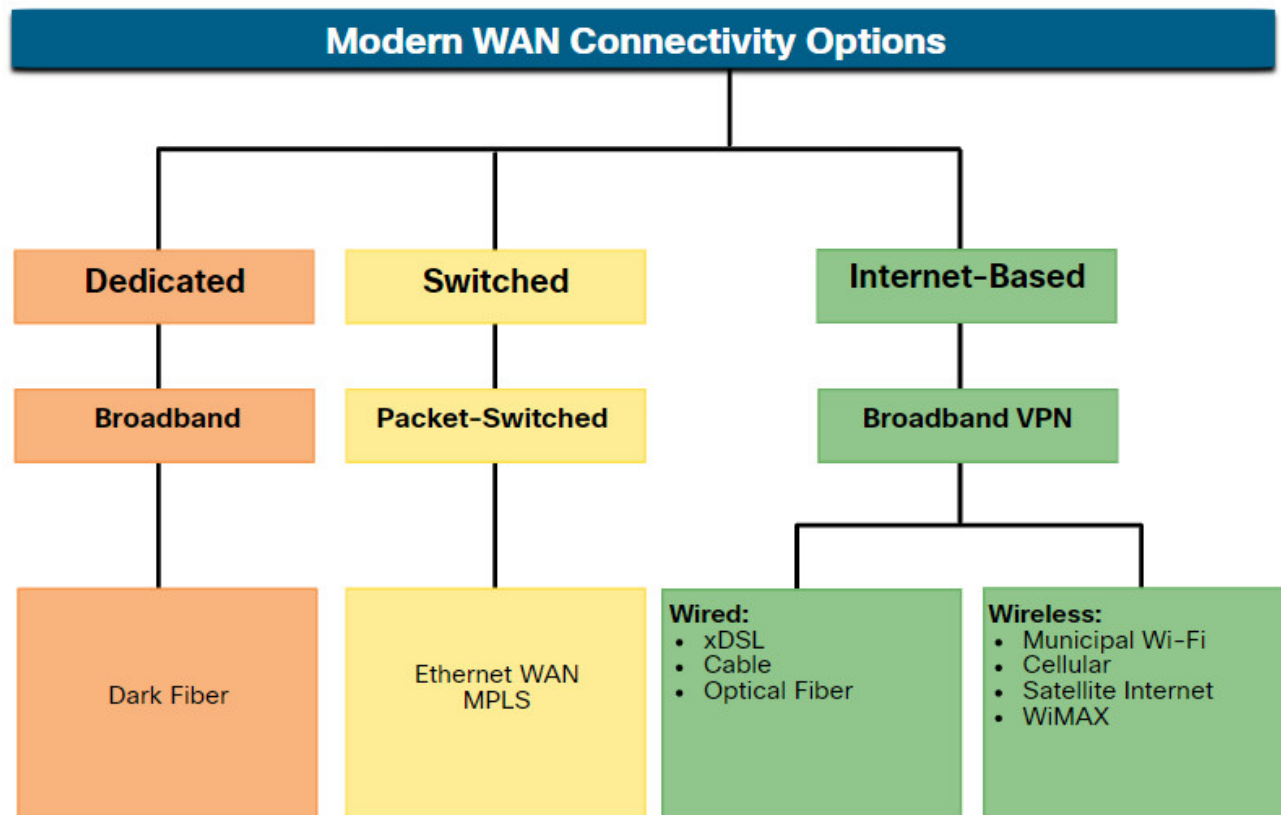


### 7.4.2. Modern WAN Connectivity Options

---



New technologies are continually emerging. The figure summarizes the modern WAN connectivity options.



Click each button for a detailed description of the three major types of modern WAN connectivity options.

- [Dedicated Broadband](#)
- [Packet-Switched](#)
- [Internet-based Broadband](#)

### **Dedicated Broadband**

In the late 1990s, many telecommunication companies built optical fiber networks with enough fiber to satisfy projected next generation needs. However, optical technologies such as wavelength division multiplexing (WDM) were developed and dramatically increased the transmitting ability of a single strand of optical fiber. Consequently, many fiber-optic cable runs are not in use. Fiber-optic cable that is not in use, and therefore, “un-lit” (i.e. dark) is referred to as dark fiber.

Fiber can be installed independently by an organization to connect remote locations directly together. However, dark fiber could also be leased or purchased from a supplier. Leasing dark fiber is typically more expensive than any other WAN option available today. However, it provides the greatest flexibility, control, speed, and security.

### **Packet-Switched**

Two packet-switched WAN network options are available.

Advances in Ethernet LAN technology have enabled it to expand into the MAN and WAN areas. Metro Ethernet provides fast bandwidth links and has been responsible for replacing many traditional WAN connectivity options.

Multi-protocol Label Switching (MPLS) enables the WAN provider network to carry any protocol (e.g., IPv4 packets, IPv6 packets, Ethernet, DSL) as payload data. This enables different sites to connect to the provider network regardless of its access technologies.

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

### 7.4.3. Ethernet WAN

---

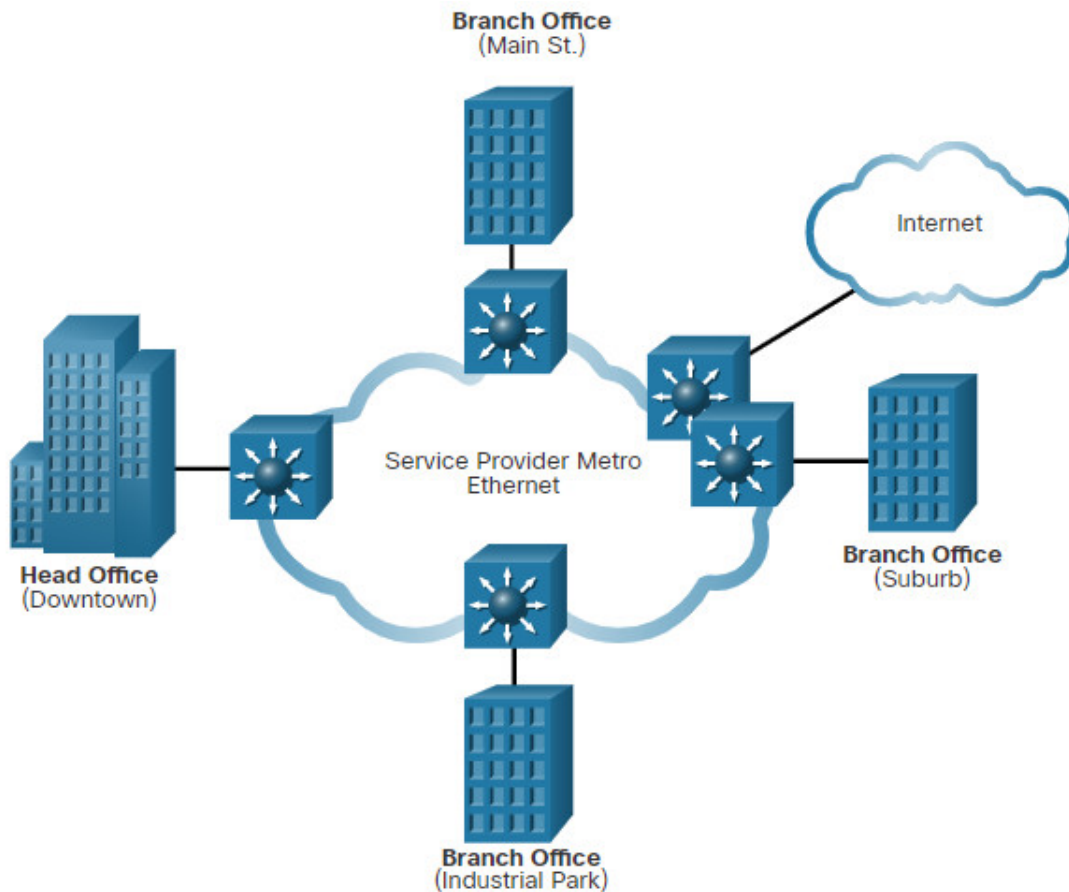
Ethernet was originally developed as a LAN access technology and was not suitable as a WAN access technology due primarily to the limited distance provided by copper media.

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 the following:

- Metropolitan Ethernet (Metro E)
- Ethernet over MPLS (EoMPLS)
- Virtual Private LAN Service (VPLS)

The figure displays a simple Metro Ethernet topology example.



The following are several benefits to an Ethernet WAN:

- **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 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.

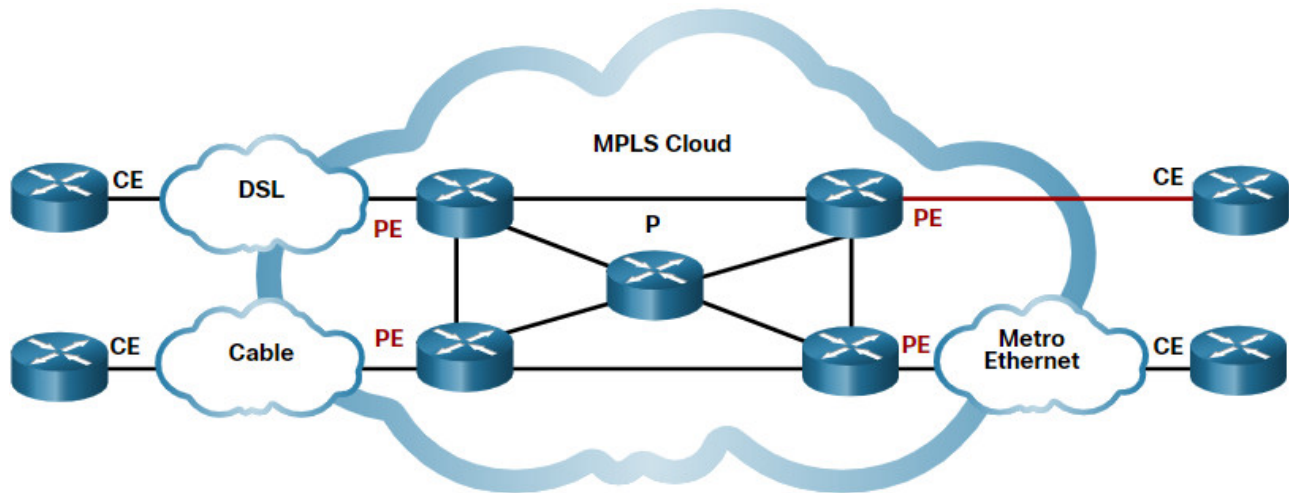
**Note:** Ethernet WANs have gained in popularity and are now commonly being used to replace the traditional serial point-to-point, Frame Relay and ATM WAN links.

#### 7.4.4. MPLS

Multiprotocol Label Switching (MPLS) is a high-performance service provider WAN routing technology to interconnect clients without regard to access method or payload. MPLS supports a variety of client access methods (e.g., Ethernet, DSL, Cable, Frame Relay). MPLS

can encapsulate all types of protocols including IPv4 and IPv6 traffic.

Refer to the sample topology of a simple MPLS enabled network.



An MPLS router can be a customer edge (CE) router, a provider edge (PE) router, or an internal provider (P) router. Notice that MPLS supports a variety of client access connections.

MPLS routers are label switched routers (LSRs). This means that they attach labels to packets that are then used by other MPLS routers to forward traffic. When traffic is leaving the CE, the MPLS PE router adds a short fixed-length label in between the frame header and packet header. MPLS P routers use the label to determine the next hop of the packet. The label is removed by the egress PE router when the packet leaves the MPLS network.

MPLS also provides services for QoS support, traffic engineering, redundancy, and VPNs.

## 7.5. Internet-Based Connectivity

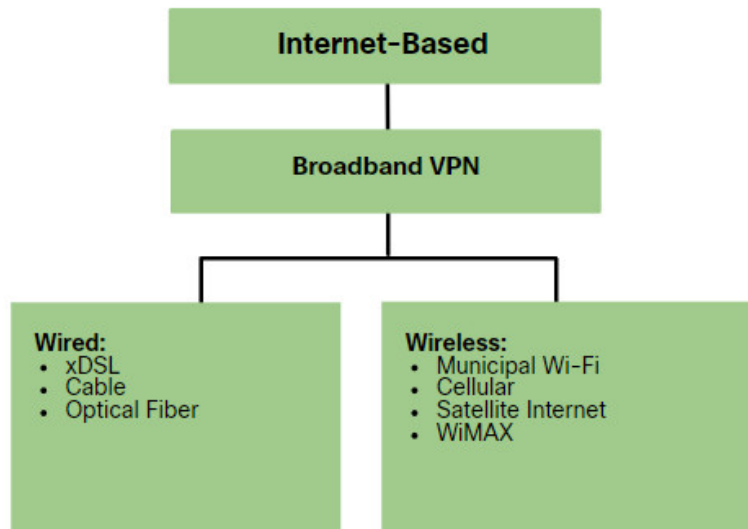
---

### 7.5.1. Internet-Based Connectivity Options

---

Modern WAN connectivity options do not end with Ethernet WAN and MPLS. Today, there are a host of internet-based wired and wireless options from which to choose. Internet-based broadband connectivity is an alternative to using dedicated WAN options.

The figure lists the internet-based connectivity options.



Internet-based connectivity can be divided into wired and wireless options.

### **Wired options**

Wired options use permanent cabling (e.g., copper or fiber) to provide consistent bandwidth, and reduce error rates and latency. Examples of wired broadband connectivity are Digital Subscriber Line (DSL), cable connections, and optical fiber networks.

### **Wireless options**

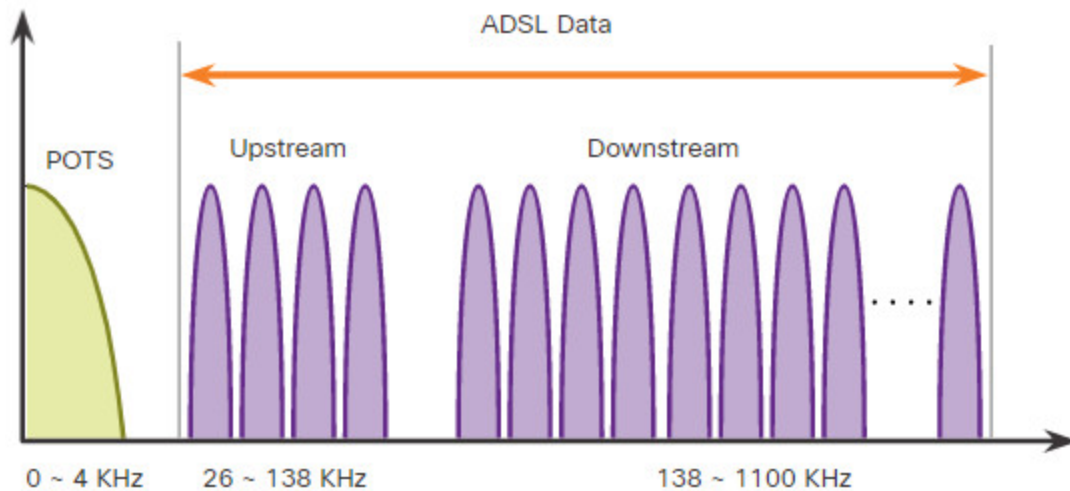
Wireless options are less expensive to implement compared to other WAN connectivity options because they use radio waves instead of wired media to transmit data. However, wireless signals can be negatively affected by factors such as distance from radio towers, interference from other sources, weather, and number of users accessing the shared space. Examples of wireless broadband include cellular 3G/4G/5G or satellite internet services. Wireless carrier options vary depending on location.

## **7.5.2. DSL Technology**

---

A Digital Subscriber Line (DSL) is a high-speed, always-on, connection technology that uses existing twisted-pair telephone lines to provide IP services to users. DSL is a popular choice for home users and for enterprise IT departments to support teleworkers.

The figure shows a representation of bandwidth space allocation on a copper wire for Asymmetric DSL (ADSL).



The area labeled POTS (Plain Old Telephone System) identifies the frequency range used by the voice-grade telephone service. The area labeled ADSL represents the frequency space used by the upstream and downstream DSL signals. The area that encompasses both the POTS area and the ADSL area represents the entire frequency range supported by the copper wire pair.

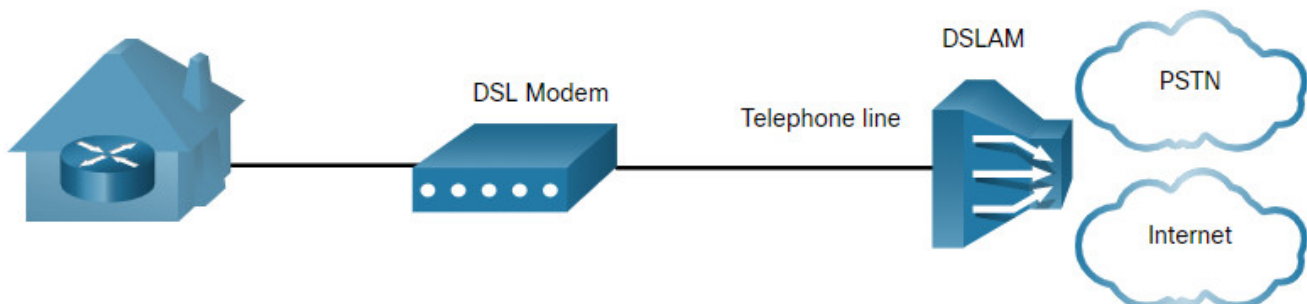
There are several xDSL varieties offering different upload and download transmission rates. However, all forms of DSL are categorized as either Asymmetric DSL (ADSL) or Symmetric DSL (SDSL). ADSL and ADSL2+ provide higher downstream bandwidth to the user than upload bandwidth. SDSL provides the same capacity in both directions.

The transfer rates are also dependent on the actual length of the local loop, and the type and condition of the cabling. For example, an ADSL loop must be less than 5.46 km (3.39 miles) for guaranteed signal quality.

Security risks are incurred in this process but can be mediated with security measures such as VPNs.

### 7.5.3. DSL Connections

Service providers deploy DSL connections in the local loop. As shown in the figure, the connection is set up between the DSL modem and the DSL access multiplexer (DSLAM).



The DSL modem converts the Ethernet signals from the teleworker device to a DSL signal, which is transmitted to a DSL access multiplexer (DSLAM) at the provider location.

A DSLAM is the device located at the Central Office (CO) of the provider and concentrates connections from multiple DSL subscribers. A DSLAM is often built into an aggregation router.

The advantage that DSL has over cable technology is that DSL is not a shared medium. Each user has a separate direct connection to the DSLAM. Adding users does not impede performance, unless the DSLAM internet connection to the ISP, or to the internet, becomes saturated.

#### **7.5.4. DSL and PPP**

---

Point-to-Point protocol (PPP) is a Layer 2 protocol that was commonly used by telephone service providers to establish router-to-router and host-to-network connections over dial-up and ISDN access networks.

ISPs still use PPP as the Layer 2 protocol for broadband DSL connections because of the following factors:

- PPP can be used to authenticate the subscriber.
- PPP can assign a public IPv4 address to the subscriber.
- PPP provides link-quality management features.

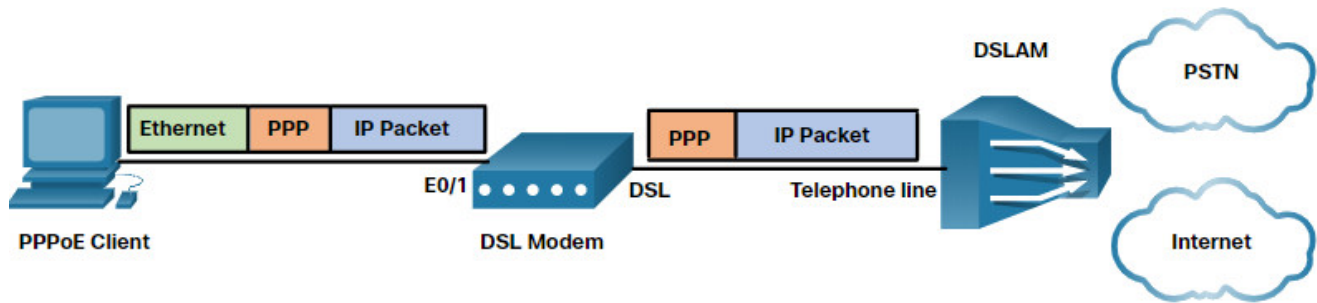
A DSL modem has a DSL interface to connect to the DSL network, and an Ethernet interface to connect to the client device. However, Ethernet links do not natively support PPP.

Click each button for an illustration and explanation of two ways PPP over Ethernet (PPPoE) can be deployed.

##### **Host with PPPoE Client**

As shown in the figure, the host runs a PPPoE client to obtain a public IP address from a PPPoE server located at the provider site. The PPPoE client software communicates with the DSL modem using PPPoE and the modem communicates with the ISP using PPP. In this topology, only one client can use the connection. Also, notice that there is no router to protect the inside network.





### 7.5.5. Cable Technology

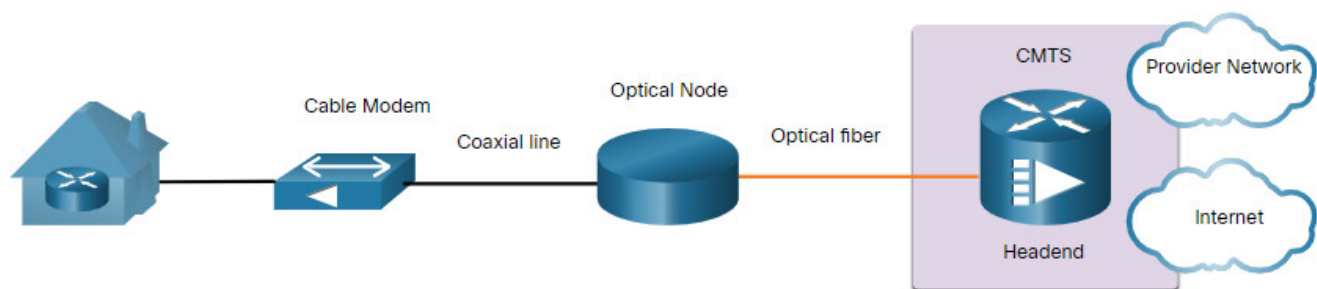
Cable technology is a high-speed always-on connection technology that uses a coaxial cable from the cable company to provide IP services to users. Like DSL, cable technology is a popular choice for home users and for enterprise IT departments to support remote workers.

Modern cable systems offer customers advanced telecommunications services, including high-speed internet access, digital cable television, and residential telephone service.

The Data over Cable Service Interface Specification (DOCSIS) is the international standard for adding high-bandwidth data to an existing cable system.

Cable operators deploy hybrid fiber-coaxial (HFC) networks to enable high-speed transmission of data to cable modems. The cable system uses a coaxial cable to carry radio frequency (RF) signals to the end user.

HFC uses fiber-optic and coaxial cable in different portions of the network. For example, the connection between the cable modem and optical node is coaxial cable, as shown in the figure.



The optical node performs optical to RF signal conversion. Specifically, it converts RF signals to light pulses over fiber-optic cable. The fiber media enables the signals to travel over long distances to the provider headend where a Cable Modem Termination System (CMTS) is located.

The headend contains the databases needed to provide internet access while the CMTS is responsible for communicating with the cable modems.

All the local subscribers share the same cable bandwidth. As more users join the service, available bandwidth may drop below the expected rate.

### 7.5.6. Optical Fiber

---

Many municipalities, cities, and providers install fiber-optic cable to the user location. This is commonly referred to as Fiber to the x (FTTx) and includes the following:

- **Fiber to the Home (FTTH)** – Fiber reaches the boundary of the residence. Passive optical networks and point-to-point Ethernet are architectures that can deliver cable TV, internet, and phone services over FTTH networks directly from an the service provider central office.
- **Fiber to the Building (FTTB)** – Fiber reaches the boundary of the building, such as the basement in a multi-dwelling unit, with the final connection to the individual living space being made via alternative means, like curb or pole technologies.
- **Fiber to the Node/Neighborhood (FTTN)** – Optical cabling reaches an optical node that converts optical signals to a format acceptable for twisted pair or coaxial cable to the premise.

FTTx can deliver the highest bandwidth of all broadband options.

### 7.5.7. Wireless Internet-Based Broadband

---

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 had a wired connection to the internet.

Click each button for a description of new developments that are enabling broadband wireless technology.

#### **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.

### 7.5.8. VPN Technology

---

Security risks are incurred when a teleworker or a remote office worker uses a broadband service to access the corporate WAN over the internet.

To address security concerns, broadband services provide Virtual Private Networks (VPN) connections to a network device that accepts VPN connections. The network device 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. VPN tunnels are routed through the internet from the private network of the company to the remote site or employee host.

The following are several benefits to using VPN:

- **Cost savings** – VPNs enable organizations to use the global internet to connect remote offices, and to connect remote users to the main corporate site. This eliminates 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 can 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. VPNs allow mobile workers and telecommuters to 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.

VPNs are commonly implemented as the following:

- **Site-to-site VPN** – VPN settings are configured on routers. Clients are unaware that their data is being encrypted.
- **Remote Access** – The user is aware and initiates remote access connection. For example, using HTTPS in a browser to connect to your bank. Alternatively, the user can run VPN client software on their host to connect to and authenticate with the destination device.

**Note:** VPNs are discussed in more detail later in this course.

### 7.5.9. ISP Connectivity Options

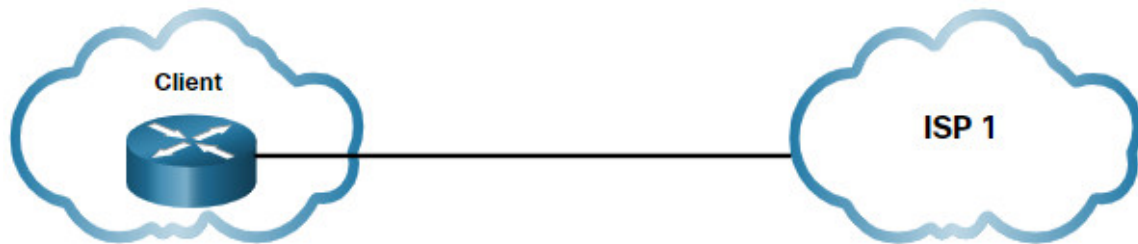
---

Click each button for an illustration and explanation about the different ways an organization can connect to an ISP. The choice depends on the needs and budget of the organization.

- Single-homed
- Dual-homed
- Multihomed
- Dual-multihomed

### Single-homed

Single-homed ISP connectivity is used by organization when internet access is not crucial to the operation. As shown in the figure, the client connects to the ISP using one link. The topology provides no redundancy. This is the least expensive solution of the four shown.



### 7.5.10. Broadband Solution Comparison

---

Each broadband solution has advantages and disadvantages. The ideal solution is to have a fiber-optic cable directly connected to the client network. Some locations have only one option, such as cable or DSL. Some locations only have broadband wireless options for internet connectivity.

If there are multiple broadband solutions available, a cost-versus-benefit analysis should be performed to determine the best solution.

Some factors to consider include the following:

- **Cable** – Bandwidth is shared by many users. Therefore, upstream data rates are often slow during high-usage hours in areas with over-subscription.
- **DSL** – Limited bandwidth that is distance sensitive (in relation to the ISP central office). Upload rate is proportionally lower compared to download rate.
- **Fiber-to-the-Home** – This option requires fiber installation directly to the home.
- **Cellular/Mobile** – With this option, coverage is often an issue, even within a small office or home office where bandwidth is relatively limited.
- **Municipal Wi-Fi** – Most municipalities do not have a mesh Wi-Fi network deployed. If it is available and in range, then it is a viable option.
- **Satellite** – This option is expensive and provides limited capacity per subscriber. Typically used when no other option is available.

### 7.5.11. Lab – Research Broadband Internet Access Options

---

In this lab, you will complete the following objectives:

- Part 1: Investigate Broadband Distribution
- Part 2: Research Broadband Access Options for Specific Scenarios

### **7.5.11 Lab – Research Broadband Internet Access Technologies**

## **7.6. Module Practice and Quiz**

---

### **7.6.1. Packet Tracer – WAN Concepts**

---

In this Packet Tracer activity, you will explore various WAN technologies and implementations.

#### **7.6.1 Packet Tracer – WAN Concepts**

### **7.6.2. What did I learn in this module?**

---

#### **Purpose of WANs**

A Wide Area Network (WAN) is required to connect beyond the boundary of the LAN. A WAN is a telecommunications network that spans over a relatively large geographical area. A WAN operates beyond the geographic scope of a LAN. A private WAN is a connection that is dedicated to a single customer. A public WAN connection is typically provided by an ISP or telecommunications service provider using the internet. WAN topologies are described using a logical topology. WANs are implemented using the following logical topologies: Point-to-Point, Hub-and-Spoke, Dual-homed, Fully Meshed, and Partially Meshed. A single-carrier connection is when an organization connects to only one service provider. A dual-carrier connection provides redundancy and increases network availability. The organization negotiates separate SLAs with two different service providers. 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. Small companies may use a single LAN connected to a wireless router to share data and peripherals.

Connection to the internet is through a broadband service provider. A slightly larger company may use a Campus Area Network (CAN). A CAN interconnects several LANs within a limited geographical area. An even larger company may require a metropolitan area network (MAN) to interconnect sites within the city. A MAN is larger than a LAN but smaller than a WAN. A global company may require teleworking and virtual teams using web-based applications, including web-conferencing, e-learning, and online collaboration tools. Site-to-site and remote access Virtual Private Networks (VPNs) enable the company to use the internet to securely connect with employees and facilities around the world.

#### **WAN Operations**

Modern WAN standards are defined and managed by a number of recognized authorities: TIA/EIA, ISO, and IEEE. Most WAN standards focus on the physical layer (OSI Layer 1) and the data link layer (OSI Layer 2). Layer 1 protocols describe the electrical, mechanical, and operational components needed to transmit bits over a WAN. Layer 1 optical fiber protocol standards include SDH, SONET, and DWDM. Layer 2 protocols define how data will be encapsulated into a frame. Layer 2 protocols include broadband, wireless, Ethernet WAN, MPLS, PPP, HDLC. The WAN physical layer describes the physical connections between the company network and the service provider network. There are specific terms used to describe WAN connections between the subscriber (i.e., the company / client) and the WAN service provider: DTE, DCE, CPE, POP, Demarcation Point, Local Loop, CO, Toll network, Backhaul network, and Backbone network. The end-to-end data path over a WAN is usually from source DTE to the DCE, then to the WAN cloud, then to the DCE to and finally to the destination DTE. Devices used in this path include voiceband modem, DSL and Cable modems, CSU/DSU, Optical converter, wireless router or access point, and other WAN core devices. Serial communication transmits bits sequentially over a single channel. In contrast, parallel communications simultaneously transmit several bits using multiple wires. A circuit-switched network establishes a dedicated circuit (or channel) between endpoints before the users can communicate. During transmission over a circuit-switched network, all communication uses the same path. The two most common types of circuit-switched WAN technologies are PSTN and ISDN. Packet-switching segments traffic data into packets that are routed over a shared network. Common types of packet-switched WAN technologies are Ethernet WAN and MPLS. There are two optical fiber OSI layer 1 standards. SDH/SONET define how to transfer multiple data, voice, and video communications over optical fiber using lasers or LEDs over great distances. Both standards are used on the ring network topology that contains redundant fiber paths allowing traffic to flow in both directions. DWDM is a newer technology that increases the data-carrying capacity SDH and SONET by simultaneously sending multiple streams of data (multiplexing) using different wavelengths of light.

## **Traditional WAN Connectivity**

In the 1980s, organizations started to see the need to interconnect their LANs with other locations. They needed their networks to connect to the local loop of a service provider by using dedicated lines or by using switched services from a service provider. When permanent dedicated connections were required, a point-to-point link using copper media was used to provide a pre-established WAN communications path from the customer premises to the provider network. Dedicated leased lines were T1/E1 or T3/E3 lines. Circuit-switched connections were provided by PSTN carriers. The local loop connecting the CPE to the CO was copper media. ISDN is a circuit-switching technology that enables the PSTN local loop to carry digital signals. This provided higher capacity switched connections than dialup access. Packet switching segments data into packets that are routed over a shared network. Packet-switching networks allow many pairs of nodes to communicate over the same channel. Frame

Relay is a simple Layer 2 NBMA WAN technology used to interconnect enterprise LANs. 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.

## **Modern WAN Connectivity**

Modern WAN connectivity options include dedicated broadband, Ethernet WAN and MPLS (packet-switched), along with various wired and wireless version of internet-based broadband. Service providers now offer Ethernet WAN service using fiber-optic cabling. Ethernet WAN reduces expenses and administration, is easily integrated with existing networks, and enhances business productivity. MPLS is a high-performance service provider WAN routing technology to interconnect clients. MPLS supports a variety of client access methods (e.g., Ethernet, DSL, Cable, Frame Relay). MPLS can encapsulate all types of protocols including IPv4 or IPv6 traffic.

## **Internet-Based Connectivity**

Internet-based broadband connectivity is an alternative to using dedicated WAN options. There are wired and wireless versions of broadband VPN. Wired options use permanent cabling e.g., copper or fiber) to provide consistent bandwidth, and reduce error rates and latency. Examples of wired broadband connectivity are Digital Subscriber Line (DSL), cable connections, and optical fiber networks. Examples of wireless broadband include cellular 3G/4G/5G or satellite internet services. DSL is a high-speed, always-on, connection technology that uses existing twisted-pair telephone lines to provide IP services to users. All forms of DSL are categorized as either ADSL or SDSL. The DSL modem converts the Ethernet signals from the teleworker device to a DSL signal, which is transmitted to a DSLAM at the provider location. The advantage that DSL has over cable technology is that DSL is not a shared medium. ISPs still use PPP as the Layer 2 protocol for broadband DSL connections. A DSL modem has a DSL interface to connect to the DSL network and an Ethernet interface to connect to the client device. Ethernet links do not natively support PPP. Cable technology is a high-speed always-on connection technology that uses a cable company coaxial cable to provide IP services to users. Cable operators deploy hybrid fiber-coaxial (HFC) networks to enable high-speed transmission of data to cable modems. The cable system uses a coaxial cable to carry radio frequency (RF) signals to the end user. Many municipalities, cities, and providers install fiber optic cable to the user location. This is commonly referred to as Fiber to the x (FTTx) and versions are FTTH, FTTB, and FTTN.

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. Newer developments in wireless technology include Municipal Wi-Fi, Cellular, Satellite internet,



and WiMAX. To address security concerns, broadband services provide capabilities for using Virtual Private Networks (VPN) connections to a network device that accepts VPN connections, 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. VPN tunnels are routed through the internet from the private network of the company to the remote site or employee host. Common VPN implementations include site-to-site and remote access. ISP connectivity options include single-homed, dual-homed, multihomed, and dual-multihomed. Cable, DSL, fiber-to-the-home, cellular/mobile, municipal Wi-Fi, and satellite internet all have advantages and disadvantages. Perform a cost-versus-benefit analysis before choosing an internet-based connectivity solution.

### **7.6.3 Module Quiz – WAN Concepts**

---

#### **Download Slide Powerpoint (PPT)**

---



CCNA 3 v7.0 Curriculum: Module 7 - WAN Concepts.pptx

1 file(s)    2.45 MB

[Download](#)

Tags:[ccna 3 v7 modules](#)