ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO

P.PORTO

REDES DE COMPUTADORES I – APRESENTAÇÃO DA UNIDADE CURICULAR

Network Topologies and Types

1. Defining a Network
2. Network Types and Characteristics
3. Networks Defined Based on Resource Location
4. Networks Defined by Topology
5. Virtual Network Concepts
6. Provider Links

Defining a Network

- A computer network is a group of interconnected computing devices, such as computers, servers, printers, routers, switches, and other hardware devices, that are linked together to enable communication and data exchange.

Defining a Network

Purpose of Networks:

- File sharing between two computers
- Video chatting between computers located in different parts of the world
- Surfing the Web (for example, to use social media sites, watch streaming video, listen to an Internet radio station, or do research for a school term paper)
- Instant messaging (IM) between computers with IM software installed
- Email
- Voice over IP (VoIP), to replace traditional telephony systems

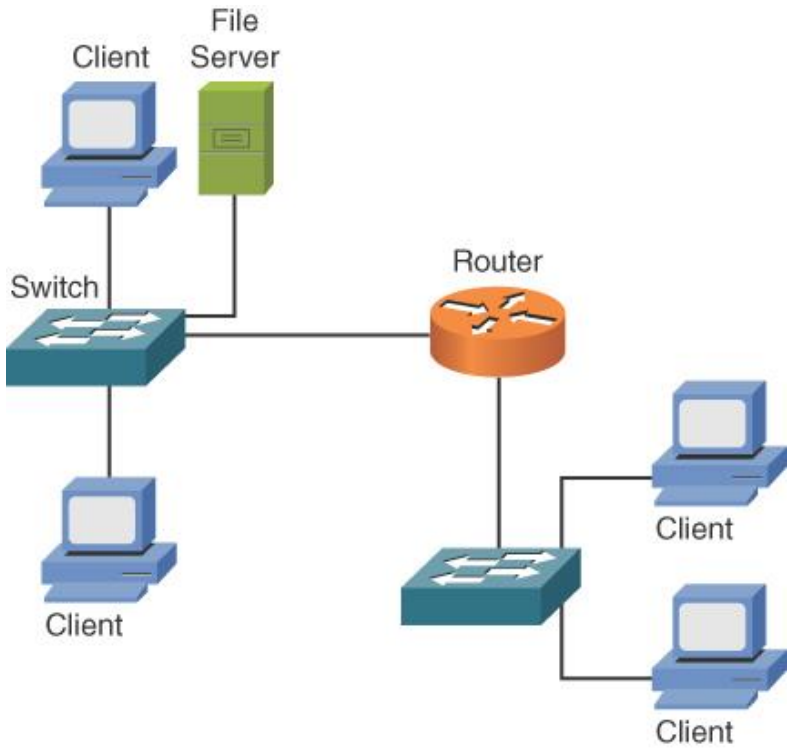
Network transporting multiple types of traffic (for example, voice, video, and data) is a *converged network*

Network Types and Characteristics

- Local area net work (LAN)
- Wide area network (WAN)
- Wireless local area network (WLAN)
- Storage area network (SAN)
- Campus area network (CAN)
- Metropolitan area network (MAN)
- Personal area network (PAN)

LAN

- Common LAN technologies
  - IEEE 802.3
  - IEEE 802.11



WAN

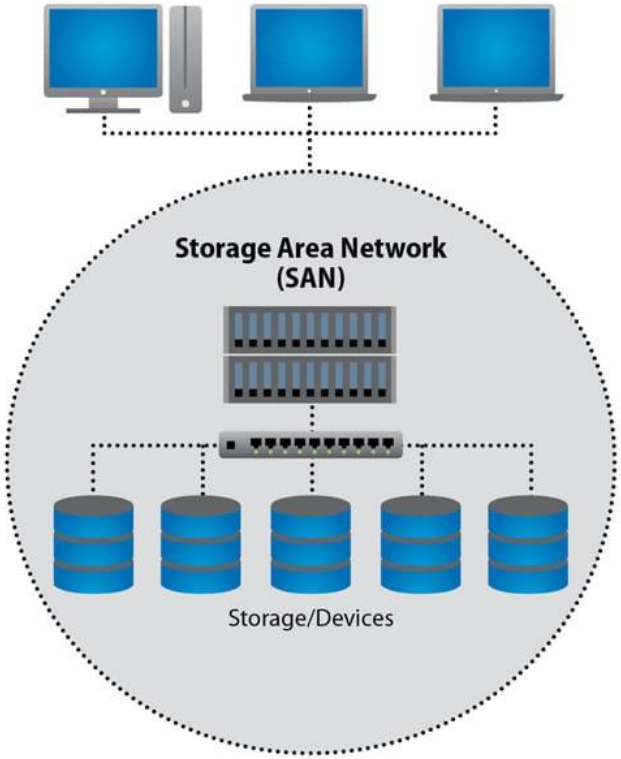
- WAN, or Wide Area Network, is a type of computer network that spans a large geographical area, typically covering multiple cities, states, or even countries. A WAN can be composed of multiple interconnected networks, such as local area networks (LANs) and metropolitan area networks (MANs), linked together using various communication technologies, such as leased lines, satellite links, or microwave connections.

WLAN

- A WLAN, Wireless Local Area Network, is a network that uses wireless communication technology, such as Wi-Fi, to connect devices within a limited geographical area, such as a home, office, or public hotspot. WLANs allow devices such as laptops, smartphones, and tablets to connect to the Internet and communicate with each other without the need for physical cables.

SAN

- A SAN, or Storage Area Network, is a network that is designed to provide high-speed access to storage devices, such as disk arrays and tape libraries to servers and applications. SANs are typically used in enterprise-level data centers and other large-scale computing environments that require high-performance, scalable, and reliable storage solutions.

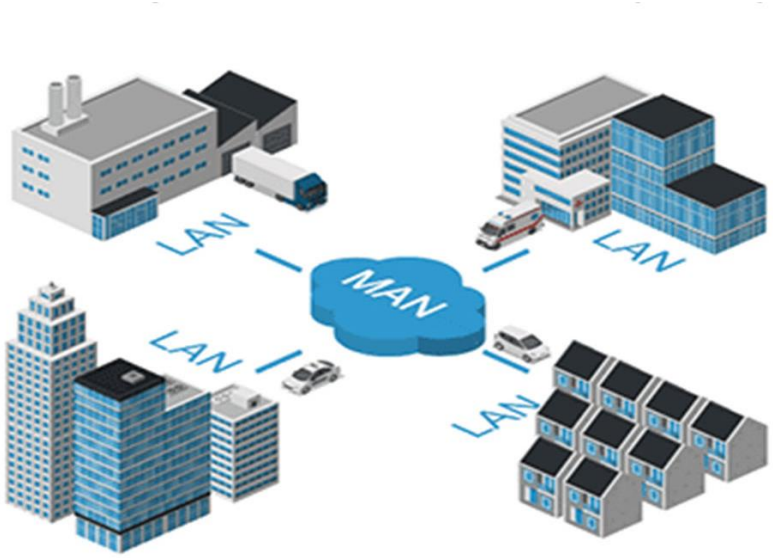


CAN

- A Campus Area Network (CAN) is a network that is designed to connect multiple buildings or locations within a relatively small geographical area, such as a university campus, corporate campus, or military base. A CAN is typically composed of multiple interconnected Local Area Networks (LANs) that are linked together using various communication technologies, such as fiber-optic cables, wireless links, or leased lines.

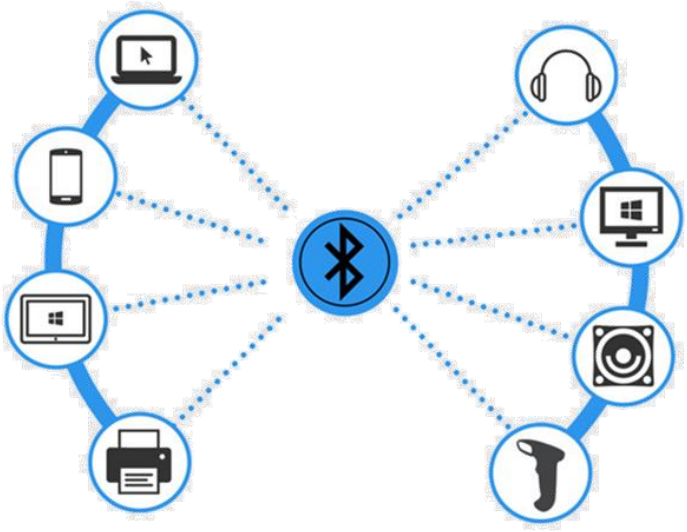
MAN

- Metropolitan Area Network (MAN) is a network that covers a geographic area larger than a Local Area Network (LAN) but smaller than a Wide Area Network (WAN). A MAN typically spans a metropolitan area, such as a city or a group of cities. A MAN may use various communication technologies, such as fiber-optic cables, wireless links, or leased lines, to connect different locations within the metropolitan area.



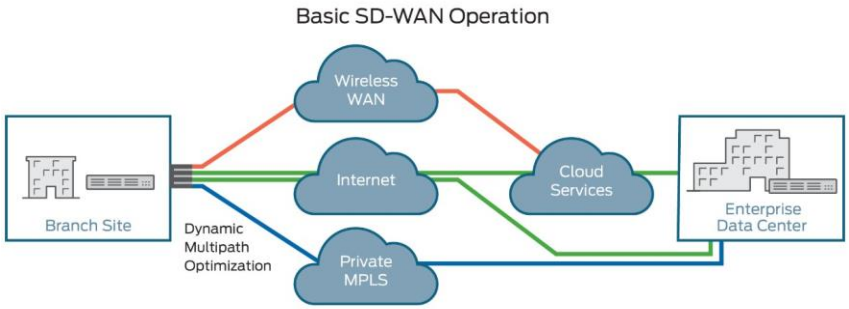
PAN

- PAN, or Personal Area Network, is a network that is designed to connect personal devices within a short range, typically within a few meters. A PAN can be formed using various communication technologies, such as Bluetooth, Infrared (IR), Near Field Communication (NFC), or Zigbee.



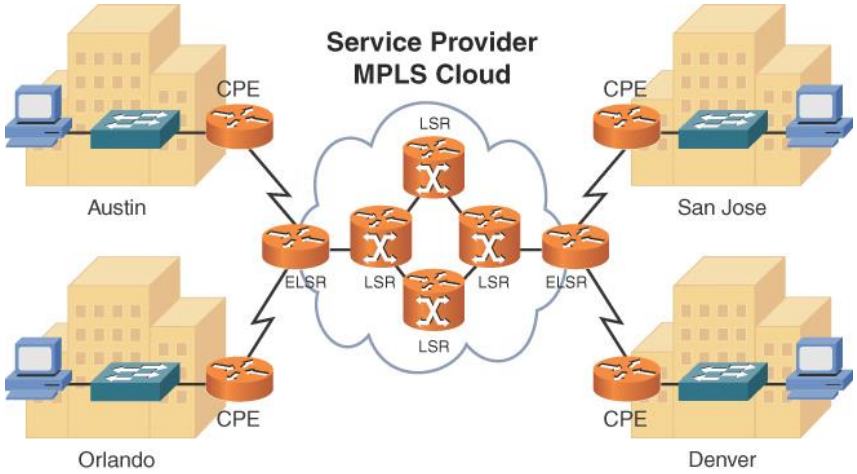
SD-WAN

- SD-WAN, or Software-Defined Wide Area Network, is network that uses software and virtualization technology to simplify and optimize the management and operation of Wide Area Networks (WANs). SD-WAN allows organizations to connect and manage multiple geographically dispersed locations, such as branch offices, data centers, and cloud services, over a single WAN.
  - SD-WAN allows organizations to manage WAN traffic more efficiently by directing traffic based on application priority, network conditions, and security policies. SD-WAN can also provide a more reliable and resilient network by using multiple transport links to ensure redundancy and failover.



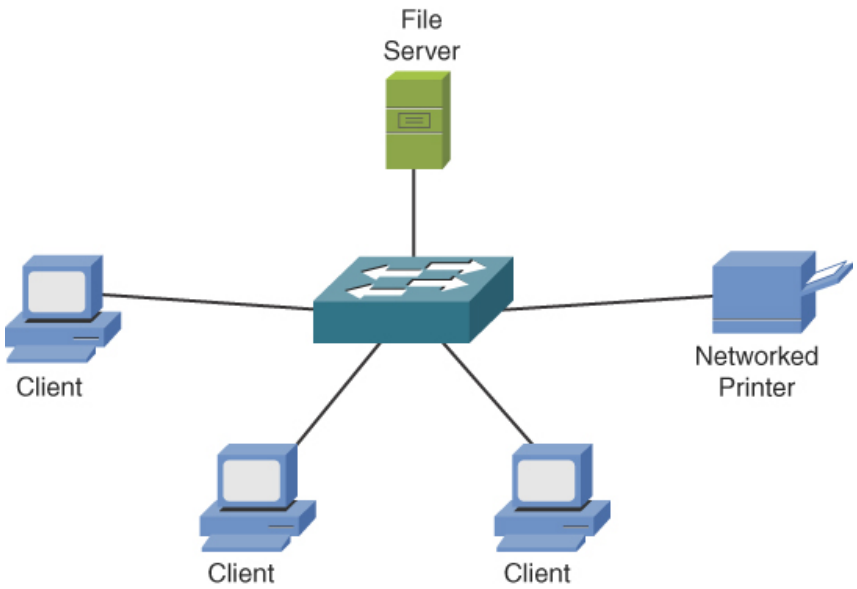
MPLS

- MPLS, or Multiprotocol Label Switching, is a networking technology that is used to improve the performance, scalability, and reliability of Wide Area Networks (WANs). MPLS allows network operators to direct and prioritize network traffic based on its type, source, and destination, using a simple and efficient label-based switching mechanism.
  - MPLS is widely used by service providers, such as telecommunications companies and Internet Service Providers (ISPs), to offer high-speed, reliable, and secure WAN connectivity to their customers. MPLS can also be used by large enterprises and organizations to build and manage their own private WANs, connecting multiple locations and cloud services.



Networks Defined Based on Resource Location – Client/Server Networks

- In this architecture, one computer or device (called the server) provides services or resources to other devices or computers (called clients) over the network. The server can be a powerful computer or a specialized device, while the clients can be desktop computers, laptops, tablets, or smartphones.
- The client devices send requests for services or resources to the server, and the server responds by providing the requested services or resources. The services provided by the server can be anything from file sharing, database access, printing services, email, web hosting, or other applications.

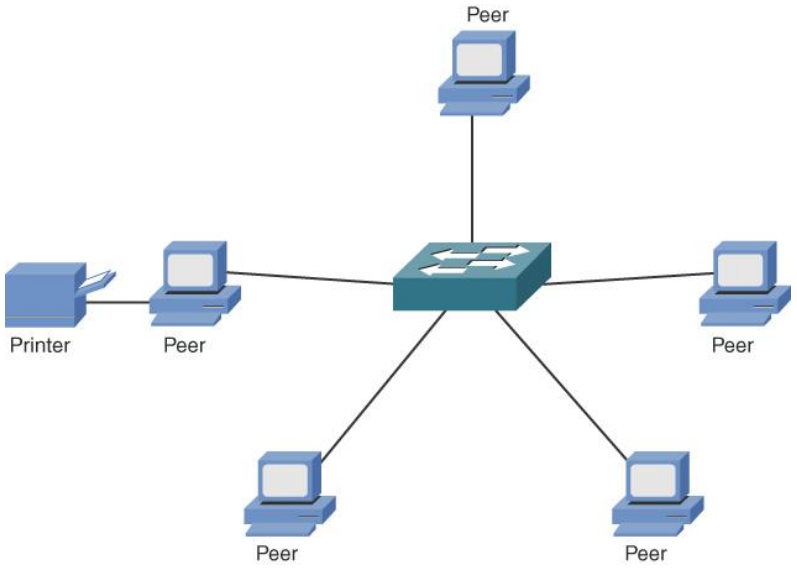


Networks Defined Based on Resource Location – Client/Server Networks

Characteristics	Benefits	Drawbacks
Client devices (for example, PCs) share a common set of resources (for example, file or print resources) located on one or more dedicated servers.	Client/server networks can easily scale, which might require the purchase of additional client licenses.	Because multiple clients might rely on a single server for their resources, the single server can become a single point of failure in the network.
Resource sharing is made possible via dedicated server hardware and network operating systems.	Administration is simplified because parameters such as file-sharing permissions and other security settings can be administered on a server as opposed to on multiple clients.	Client/server networks can cost more than peer-to-peer networks. For example, client/server networks might require the purchase of dedicated server hardware and a network OS with an appropriate number of licenses.

Networks Defined Based on Resource Location – Peer-to-Peer Networks

- A peer-to-peer (P2P) network is a distributed computing architecture where computers or devices on the network share resources and data directly with each other without the need for a central server or authority. In a P2P network, each computer or device can act as both a client and a server.



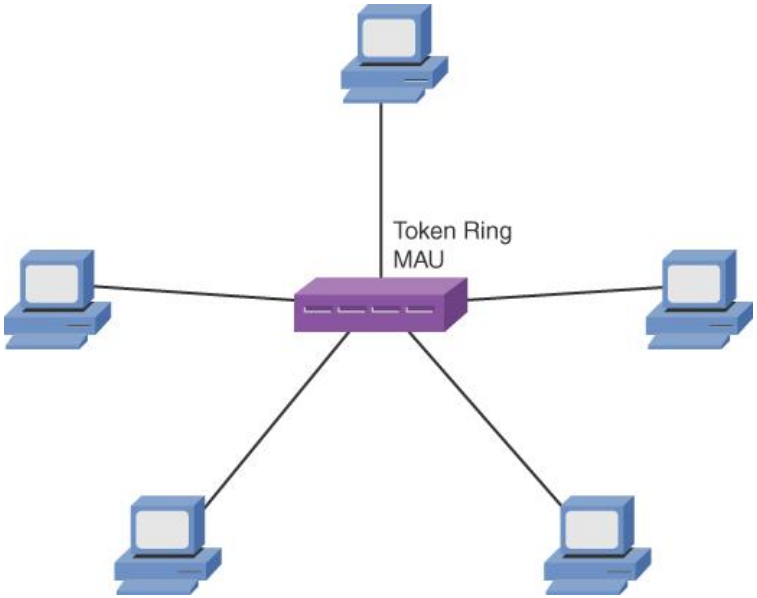
Networks Defined Based on Resource Location – Peer-to-Peer Networks

Characteristics	Benefits	Drawbacks
Client devices (for example, PCs) share their resources (for example, file and printer resources) with other client devices.	Peer-to-peer networks can be installed easily because resource sharing is made possible by the clients' operating systems, and knowledge of advanced networking operating systems is not required.	Scalability is limited because of the increased administration burden of managing multiple clients.
Resource sharing is made available through the clients' operating systems.	Peer-to-peer networks usually cost less than client/server networks because there is no requirement for dedicated server resources or advanced NOS software.	Performance might not be as strong as in a client/server network because the devices providing network resources might be performing other tasks not related to resource sharing (for example, word processing).

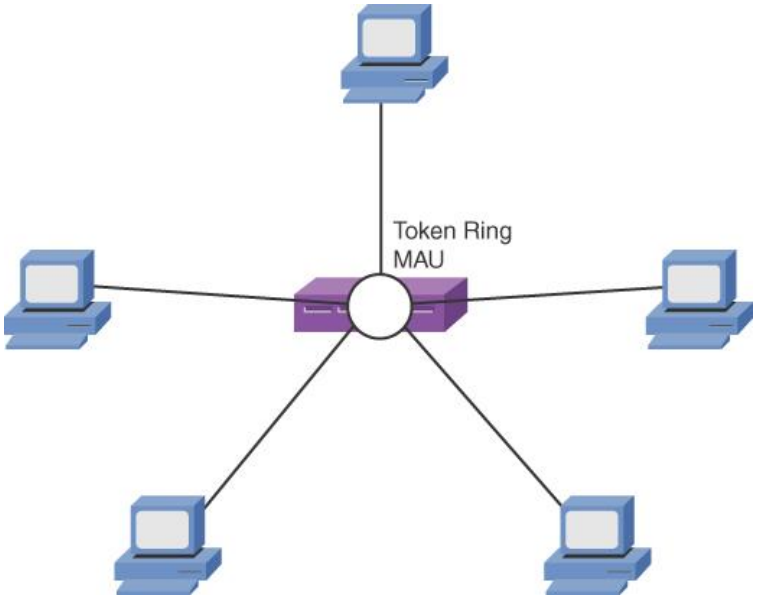
Networks Defined by Topology
Physical Versus Logical Topology

- Logical topology network refers to the way that devices on a network communicate with each other through the use of network protocols and addressing schemes. It defines the path that data takes as it flows through the network and the logical connections between devices.
- Physical topology A network topology (typically a diagram) based on how the components are physically interconnected.

Networks Defined by Topology
Physical Versus Logical Topology



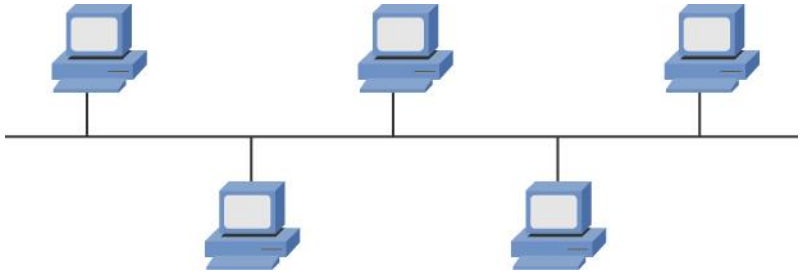
Physical topology



Logical topology
Token Ring media access unit (MAU)

Networks Defined by Topology
Bus Topology

- A bus topology is a type of network topology in which all devices are connected to a single communication path or cable called the bus. In a bus topology, each device is connected directly to the bus and can transmit data to any other device on the network by broadcasting it over the bus.
- Early Ethernet networks relied on bus topologies.

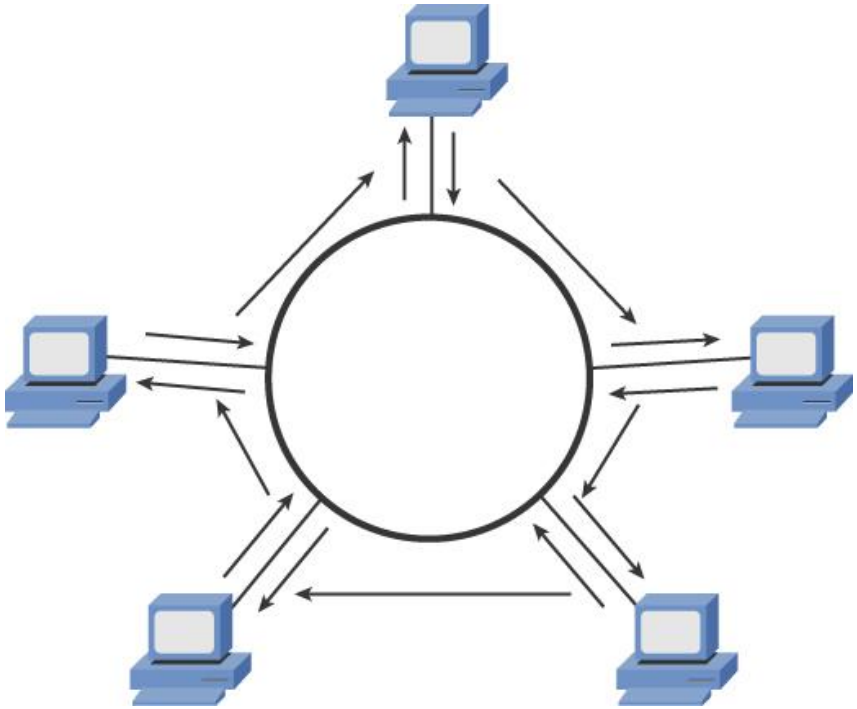


Networks Defined by Topology
Bus Topology

Characteristics	Benefits	Drawbacks
One cable is used per network segment.	Less cable is needed to install a bus topology than is required with other topologies.	Because a single cable is used per network segment, the cable is potentially a single point of failure.
To support appropriate electrical characteristics of the cable, the cable requires a terminator (of a specific resistance) at each end of the cable.	Depending on the media used by the bus, a bus topology can be less expensive than other topologies.	Troubleshooting a bus topology can be difficult because problem isolation might require inspection of multiple network taps to make sure they either have a device connected or are properly terminated.
Bus topologies were popular in early Ethernet networks.	Installation of a network based on a bus topology is easier than with some other topologies, which might require extra wiring to be installed.	Adding devices to a bus might cause an outage for other users on the bus.

Networks Defined by Topology
Ring Topology

- Ring topology In network topology in which traffic flows in a circular fashion around a closed network loop (that is, a ring). Typically, a ring topology sends data, in a single direction, to each connected device in turn, until the intended destination receives the data.

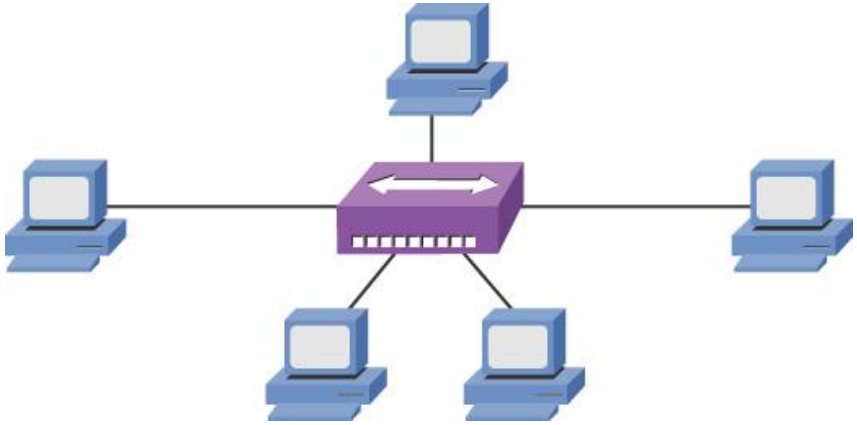


Networks Defined by Topology
Ring Topology

Characteristics	Benefits	Drawbacks
Devices are interconnected by connecting to a single ring or, in some cases (such as with FDDI), a dual ring.	A dual-ring topology adds a layer of fault tolerance. Therefore, if a cable break occurs, connectivity to all devices can be restored.	A break in a ring when a single ring topology is used results in a network outage for all devices connected to the ring.
Each device on a ring includes both a receiver (for the incoming cable) and a transmitter (for the outgoing cable).	Troubleshooting is simplified in the event of a cable break because each device on a ring contains a repeater. When the repeater on the far side of a cable break does not receive any data within a certain amount of time, it reports an error condition, typically in the form of an indicator light on a network interface card (NIC).	Rings have scalability limitations. Specifically, a ring has a maximum length and a maximum number of attached stations. Once either of these limits is exceeded, a single ring might need to be divided into two interconnected rings. A network maintenance window might need to be scheduled to perform this ring division.
Each device on the ring repeats the signal it receives.	—	Because a ring must be a complete loop, the amount of cable required for a ring is usually higher than the amount of cable required for a bus topology serving the same number of devices.

Networks Defined by Topology
Star Topology

- Star topology A network topology that has a central point (for example, a switch) from which all attached devices radiate.
- The star topology is the most popular physical LAN topology in use today, with an Ethernet switch at the center of the star and unshielded twisted-pair (UTP) cable used to connect from the switch ports to clients.

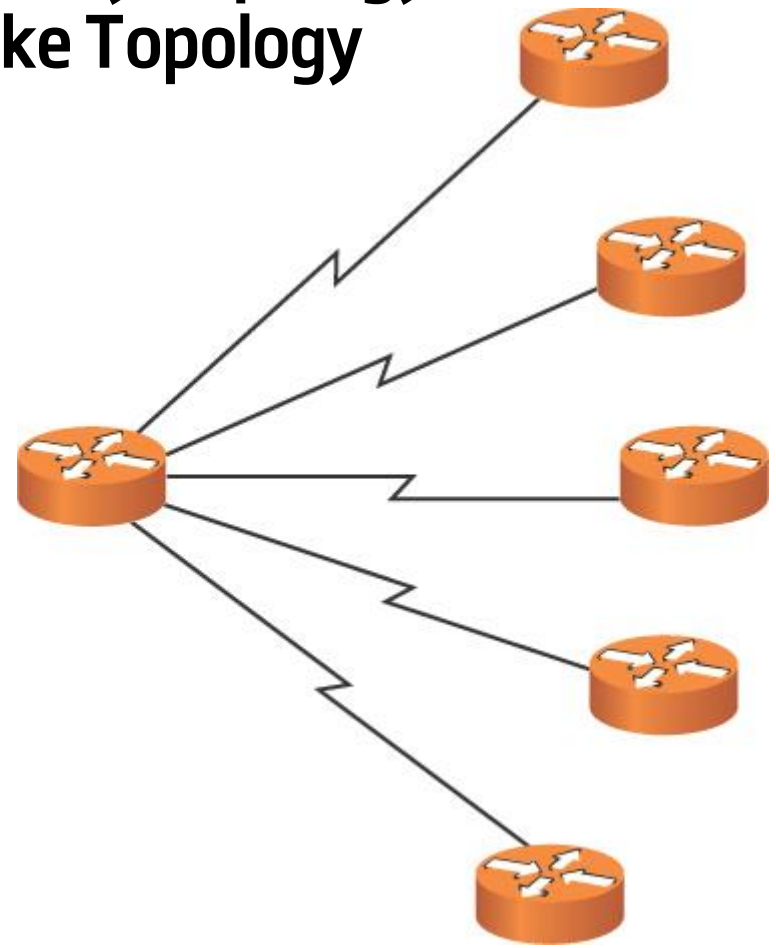


Networks Defined by Topology
Star Topology

Characteristics	Benefits	Drawbacks
Devices have independent connections to a central device (for example, a hub or a switch).	A cable break impacts only the device connected via the broken cable and not the entire topology.	More cable is required for a star topology than for bus or ring topologies because each device requires its own cable to connect back to the central device.
Star topologies are commonly used with Ethernet technologies	Troubleshooting is relatively simple because a central device in the star topology acts as the aggregation point for all the connected devices.	Installation can take longer for a star topology than for a bus or ring topology because more cable runs must be installed.

Networks Defined by Topology
Hub-and-Spoke Topology

- hub-and-spoke topology A network topology used to interconnect multiple sites (for example, multiple corporate locations) via WAN links, with a WAN link from each remote site (a spoke site) to the main site (the hub site).

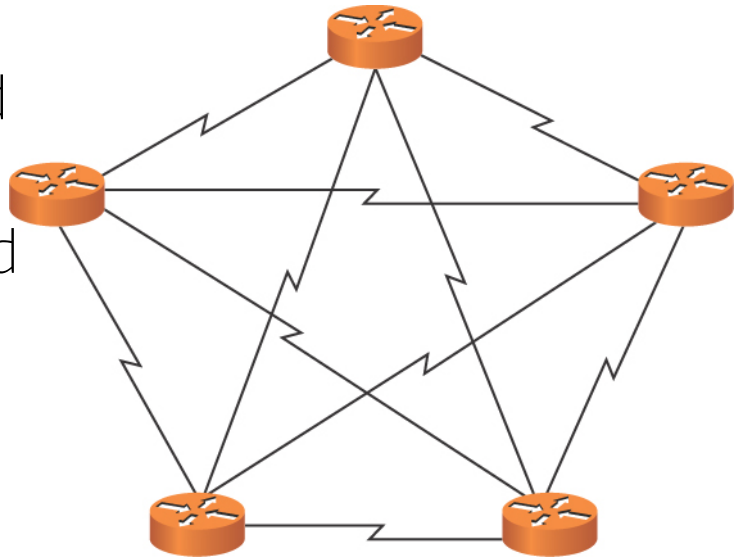


Networks Defined by Topology
Hub-and-Spoke Topology

Characteristics	Benefits	Drawbacks
Each remote site (that is, a spoke) connects to a main site (that is, the hub) via a WAN link.	Costs are reduced (as compared to with a full-mesh or partial-mesh topology) because a minimal number of links is used.	Suboptimal routes must be used between remote sites because all intersite communication must travel via the main site.
Communication between two remote sites travels through the hub site.	Adding one or more additional sites is easy (compared to in a full-mesh or partial-mesh topology) because only one link needs to be added per site.	Because all remote sites converge on the main site, this hub site is potentially a single point of failure.

Networks Defined by Topology
Full-Mesh Topology

- **hub-and-spoke topology** network topology in which every node (computer, device, or network equipment) is directly connected to every other node in the system
- Full-mesh topology can be expensive and complex to implement and manage, particularly as the number of nodes increases. This is due to the increased number of connections and associated hardware, as well as the complexity of maintaining and troubleshooting the network.

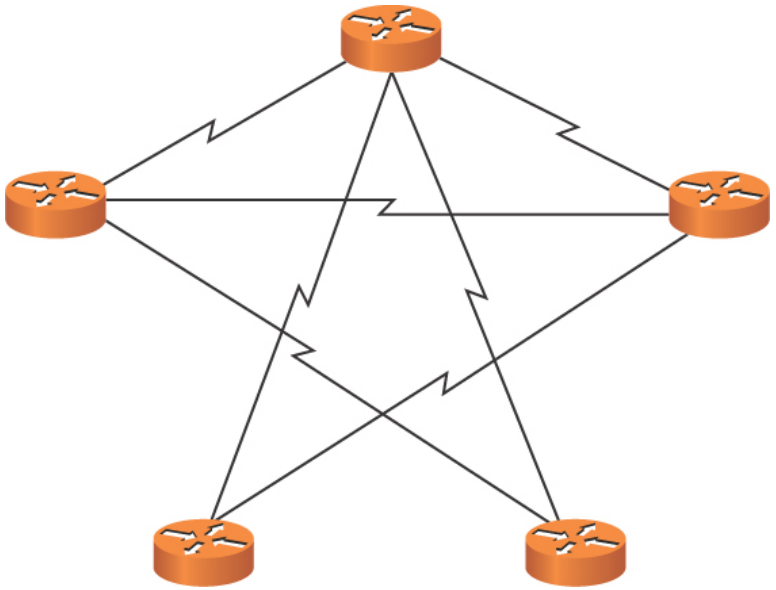


Networks Defined by Topology
Hub-and-Spoke Topology

Characteristics	Benefits	Drawbacks
Every site has a direct WAN connection to every other site.	An optimal route exists between any two sites.	A full-mesh network can be difficult and expensive to scale because the addition of one new site requires a new WAN link between the new site and every other existing site.
The number of required WAN connections can be calculated with the formula $w = n \times (n - 1) / 2$, where w = the number of WAN links and n = the number of sites. For example, a network with 10 sites would require 45 WAN connections to form a fully meshed network: $45 = 10 \times (10 - 1) / 2$.	A full-mesh network is fault tolerant because one or more links can be lost, and reachability between all sites might still be maintained.	—
—	Troubleshooting a full-mesh network is relatively easy because each link is independent of the other links.	—

Networks Defined by Topology
Partial-Mesh Topology

- partial-mesh topology A hybrid of a hub-and-spoke topology and a full-mesh topology that can be designed to provide an optimal route between selected sites, while avoiding the expense of interconnecting every site to every other site.

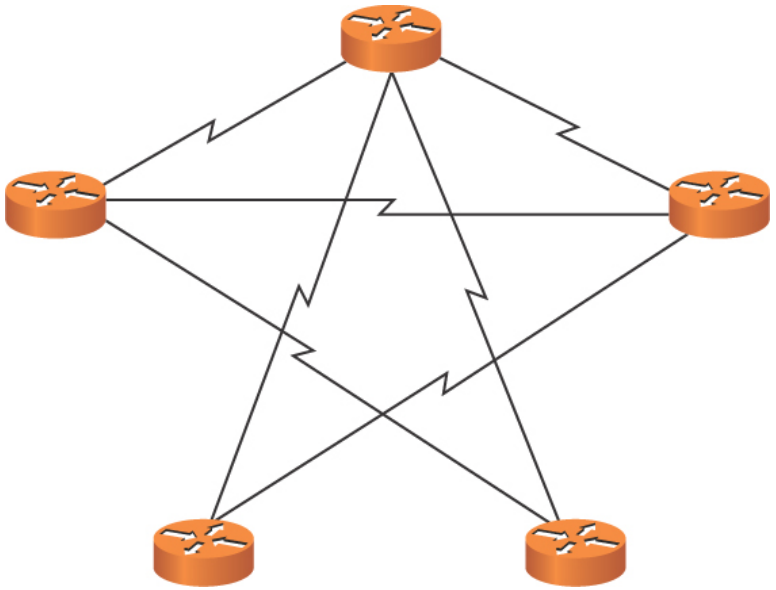


Networks Defined by Topology
Hub-and-Spoke Topology

Characteristics	Benefits	Drawbacks
Selected sites (that is, sites with frequent intersite communication) are interconnected via direct links, whereas sites that have less-frequent communication can communicate via another site.	A partial-mesh topology provides optimal routes between selected sites with higher intersite traffic volumes while avoiding the expense of interconnecting every site to every other site.	A partial-mesh topology is less fault tolerant than a full-mesh topology.
A partial-mesh topology uses fewer links than a full-mesh topology and more links than a hub-and-spoke topology for interconnecting the same number of sites.	A partial-mesh topology is more redundant than a hub-and-spoke topology.	A partial-mesh topology is more expensive than a hub-and-spoke topology.

Networks Defined by Topology
Partial-Mesh Topology

- partial-mesh topology A hybrid of a hub-and-spoke topology and a full-mesh topology that can be designed to provide an optimal route between selected sites, while avoiding the expense of interconnecting every site to every other site.

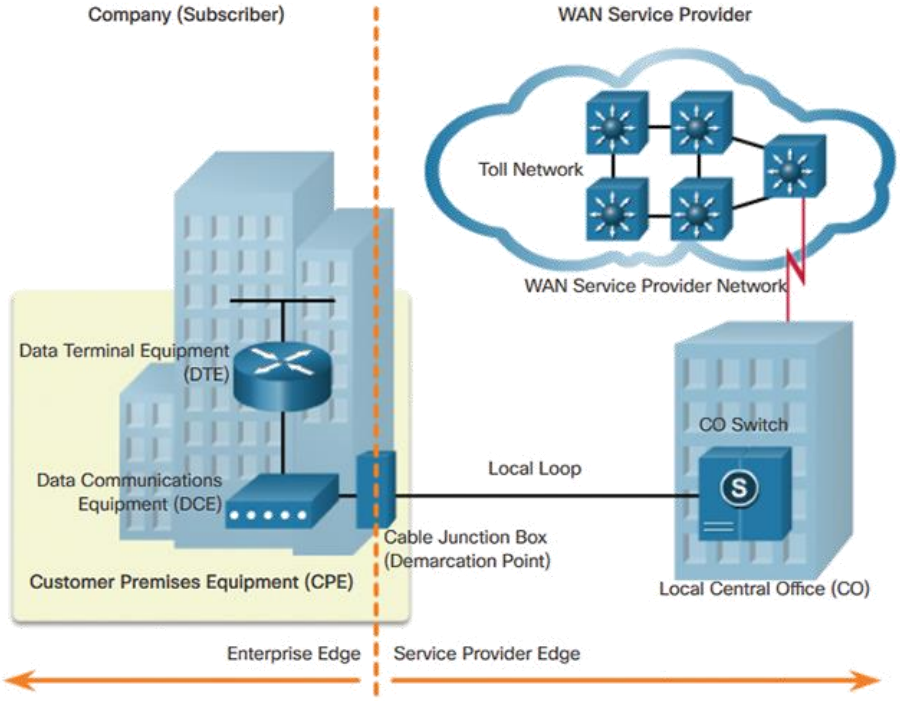


Networks Defined by Topology
Hub-and-Spoke Topology

Characteristics	Benefits	Drawbacks
Selected sites (that is, sites with frequent intersite communication) are interconnected via direct links, whereas sites that have less-frequent communication can communicate via another site.	A partial-mesh topology provides optimal routes between selected sites with higher intersite traffic volumes while avoiding the expense of interconnecting every site to every other site.	A partial-mesh topology is less fault tolerant than a full-mesh topology.
A partial-mesh topology uses fewer links than a full-mesh topology and more links than a hub-and-spoke topology for interconnecting the same number of sites.	A partial-mesh topology is more redundant than a hub-and-spoke topology.	A partial-mesh topology is more expensive than a hub-and-spoke topology.

Demarcation Point

- A demarcation point (also known as a demarc or a demarc extension) is the point in a telephone network where the maintenance responsibility passes from a telephone company to the subscriber (unless the subscriber has purchased inside wiring maintenance). This demarc is typically located in a box mounted to the outside of a customer's building (for example, a residential home). This box is called a network interface device (NID).

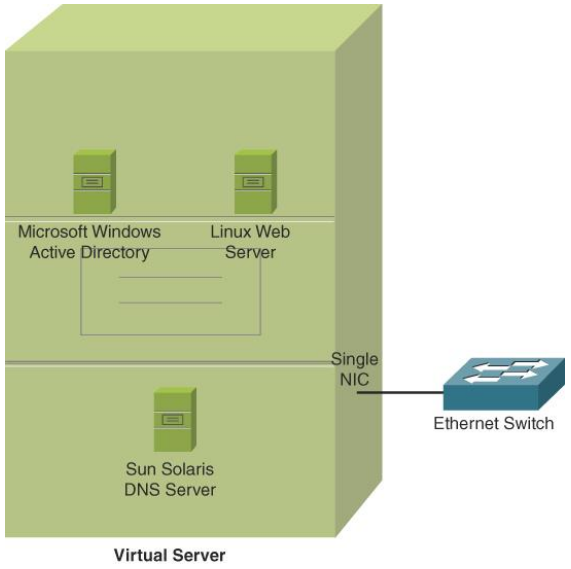


Virtual Network Concepts

- A virtual network is a computer network that is created using software rather than hardware. It is a simulated network that allows virtual machines, containers, and other virtualized resources to communicate with each other and with external networks as if they were connected to a physical network.
- Virtualization: Virtualization refers to the creation of virtual resources, such as virtual machines, virtual switches, virtual routers, and virtual firewalls, that can run on a physical server or in a cloud environment. Virtualization allows multiple virtual resources to run on the same physical hardware, which can reduce costs and increase efficiency.

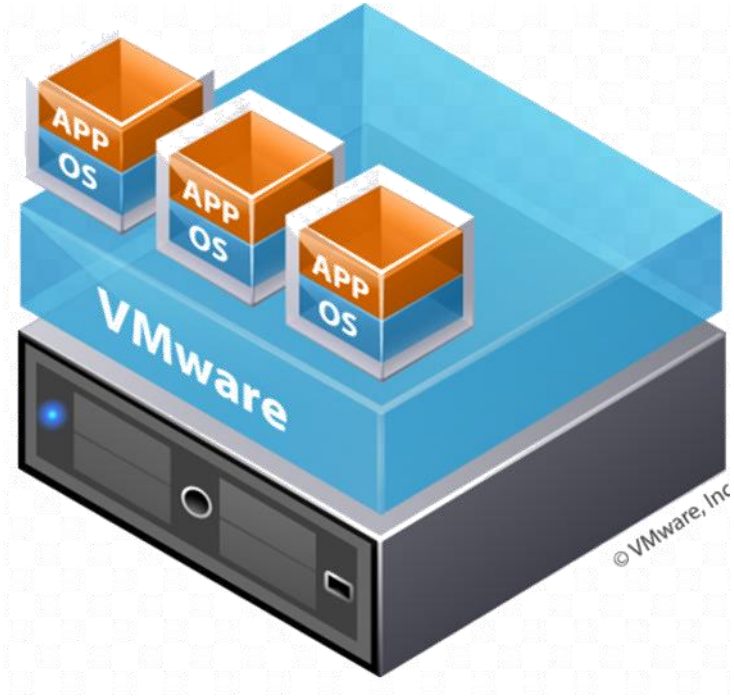
Virtual Network Concepts
Virtual Servers

- A virtual server or virtual machine, is a software-based server that runs on a physical server or in a cloud environment. It is created by using virtualization technology to partition a physical server into multiple virtual machines, each running its own operating system and applications. Each virtual machine acts as a separate server with its own resources, including CPU, memory, storage, and network connectivity.



Virtual Network Concepts
Hypervisor

- Hypervisor: A hypervisor is a piece of software that creates and manages virtual machines. It allows multiple virtual machines to run on a single physical machine, with each virtual machine running its own operating system and applications.

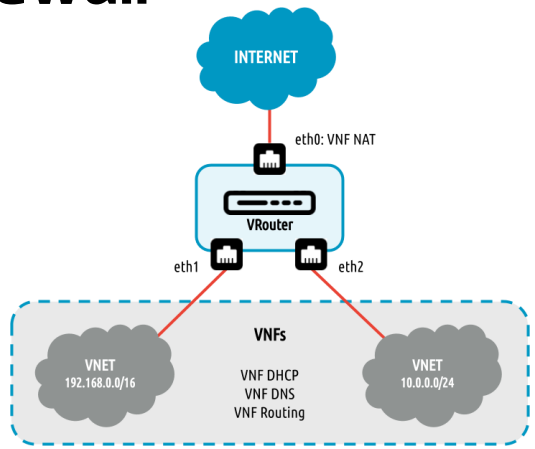


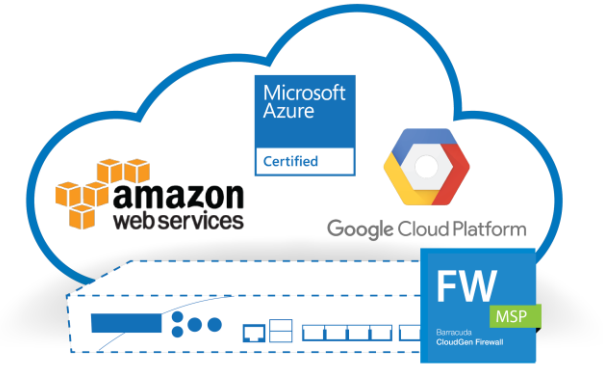
Virtual Network Concepts
Hypervisor

- Type 1 Hypervisor or Bare-Metal Hypervisor: A type 1 hypervisor is installed directly on the physical server hardware, without the need for a host operating system. It is sometimes called a bare-metal hypervisor. Type 1 hypervisors have direct access to the physical hardware and can provide better performance and security than type 2 hypervisors. Examples of type 1 hypervisors include VMware ESXi, Microsoft Hyper-V, and Citrix XenServer.
- Type 2 Hypervisor or Hosted Hypervisor: A type 2 hypervisor is installed on top of an existing operating system, such as Windows or Linux. It runs as a process within the host operating system and provides virtualization services to guest operating systems. Type 2 hypervisors are easier to install and use than type 1 hypervisors but can be less efficient and secure. Examples of type 2 hypervisors include Oracle VirtualBox, VMware Workstation, and Parallels Desktop.

Virtual Network Concepts
Virtual Router Virtual Fiorewall

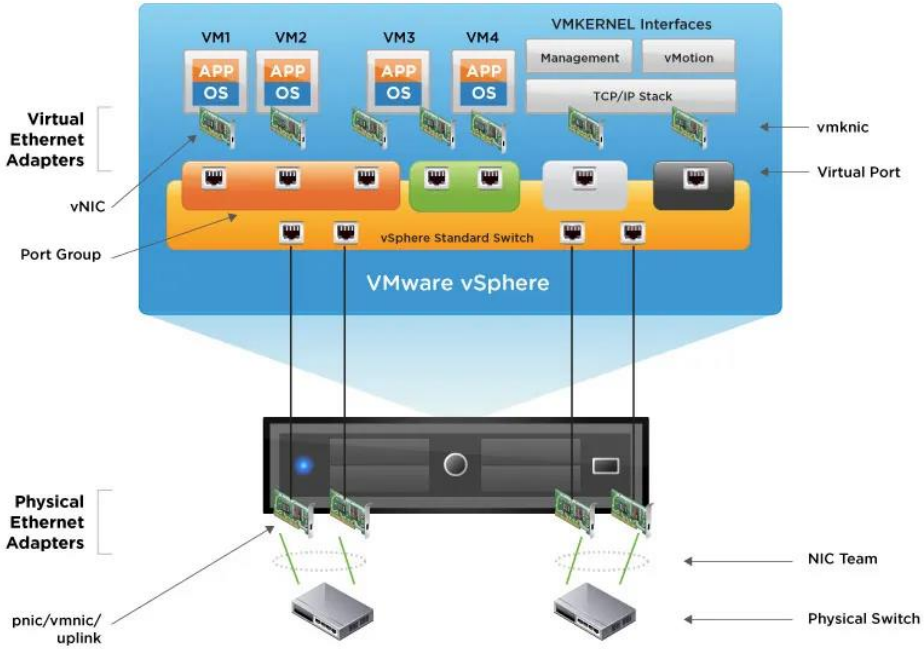
- **Virtual Router**: A virtual router is a software-based router that provides routing and forwarding functions for virtual networks. It allows virtual machines to communicate with each other and with external networks.
- **Virtual Firewall**: A virtual firewall is a software-based firewall that provides security functions for virtual networks. It allows virtual machines to be protected from external threats and provides network segmentation to control traffic flow.





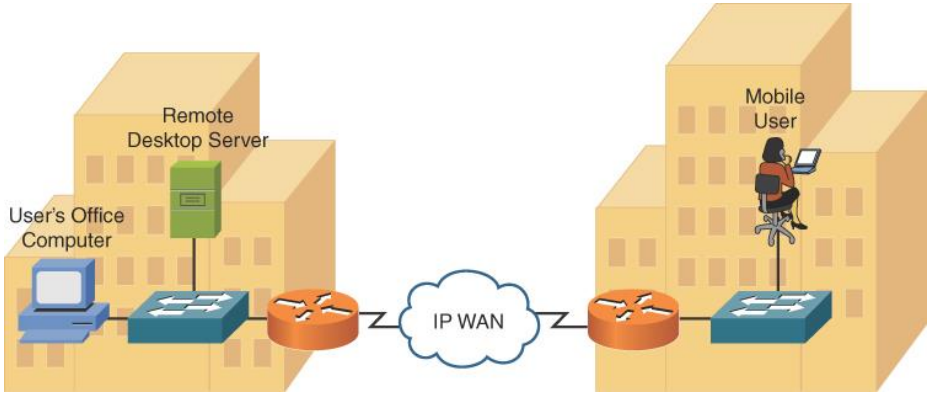
Virtual Network Concepts
Virtual Switches (vSwitches)

- **Virtual Switch**: A virtual switch is a software-based network switch that connects virtual machines and other virtualized resources. It allows virtual machines to communicate with each other and with external networks.



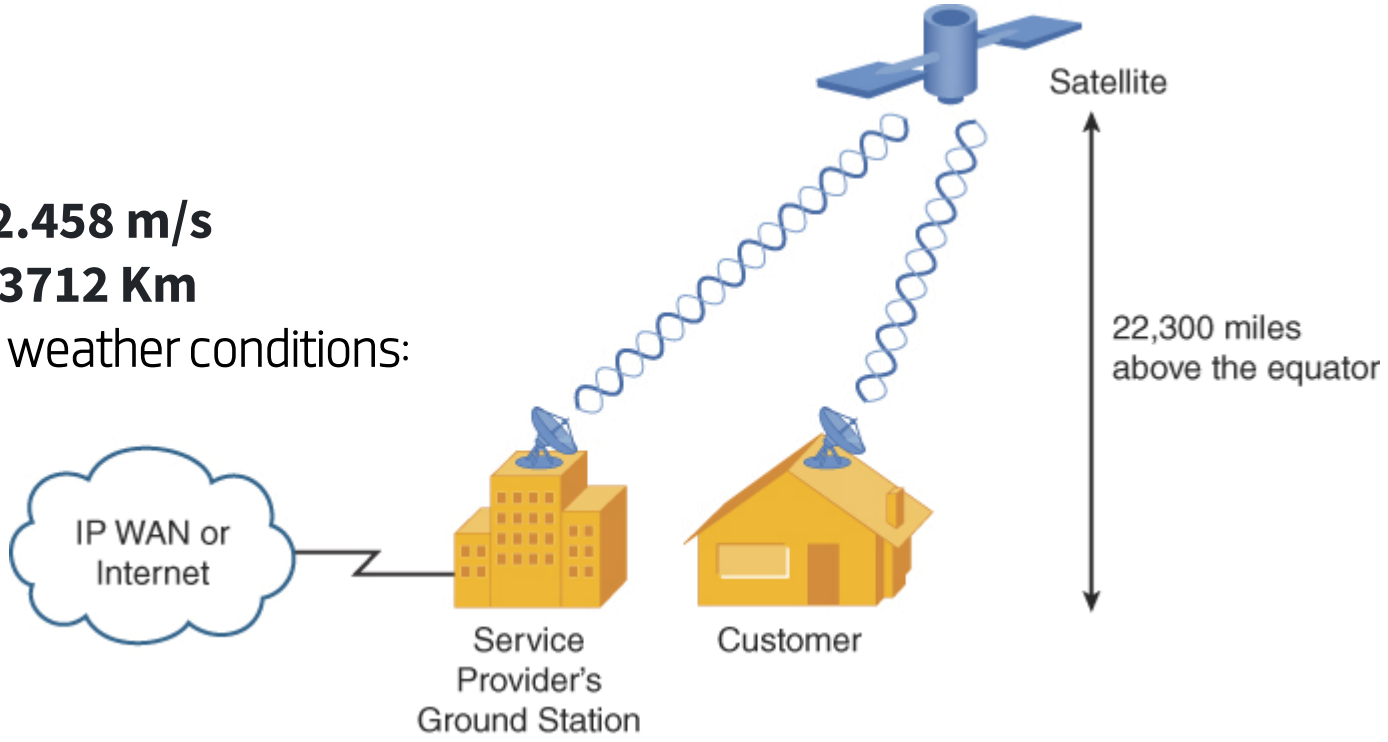
Virtual Network Concepts
Virtual Desktops

- **Virtual desktop** is a desktop environment that is hosted on a remote server and accessed remotely by users using a client device, such as a desktop computer, laptop, or mobile device. Virtual desktops are created by using virtualization technology to run multiple instances of a desktop operating system, such as Windows or Linux, on a server. Each instance of the operating system is isolated from the others, allowing multiple users to access their own virtual desktops on the same server.



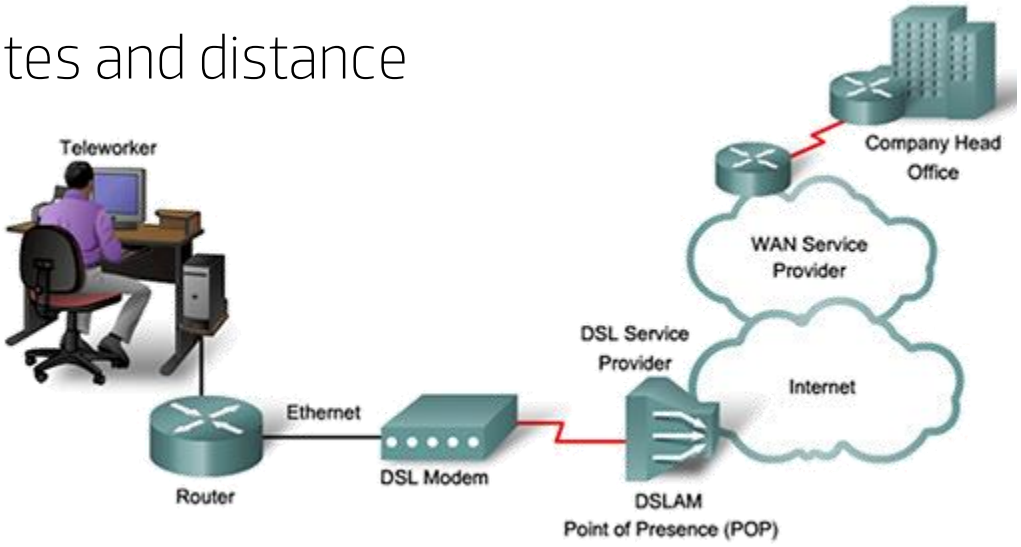
Provider Links
Satellite

- Considerations:
  - Delay:
    - **299.792.458 m/s**
    - **35 888.3712 Km**
  - Sensitivity to weather conditions:



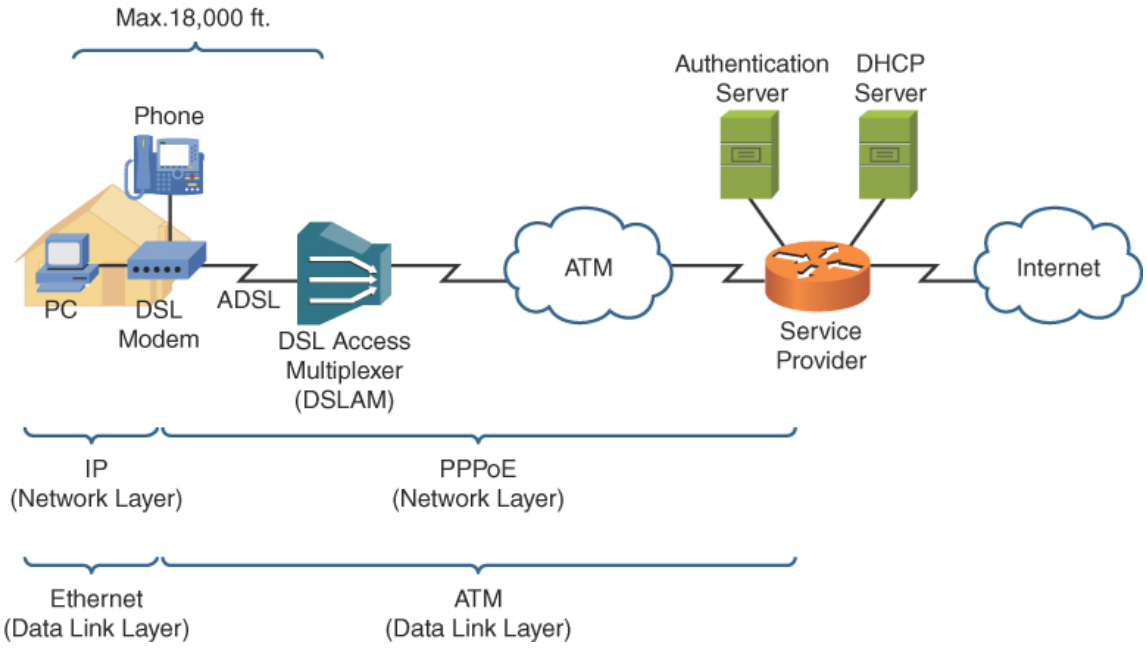
Provider Links
Digital Subscriber Line

- **digital subscriber line (DSL)** A group of technologies that provide high-speed data transmission over existing telephone wiring. DSL has several variants that differ in terms of data rates and distance limitations.



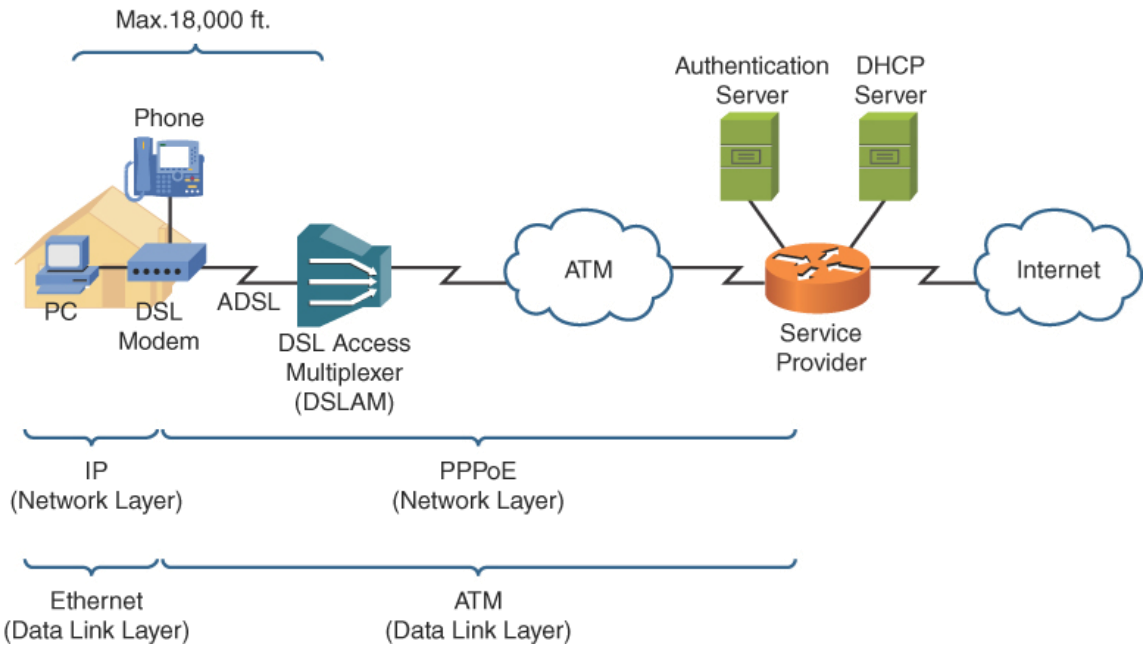
Provider Links
Digital Subscriber Line

- Asymmetric DSL (ADSL)
  - 5.4864 kilometers
    - DSL MODEM-DSLAM
  - Theoretical maximum downstream speed for an ADSL connection is 8Mbps, and the maximum upstream speed is 1.544Mbps



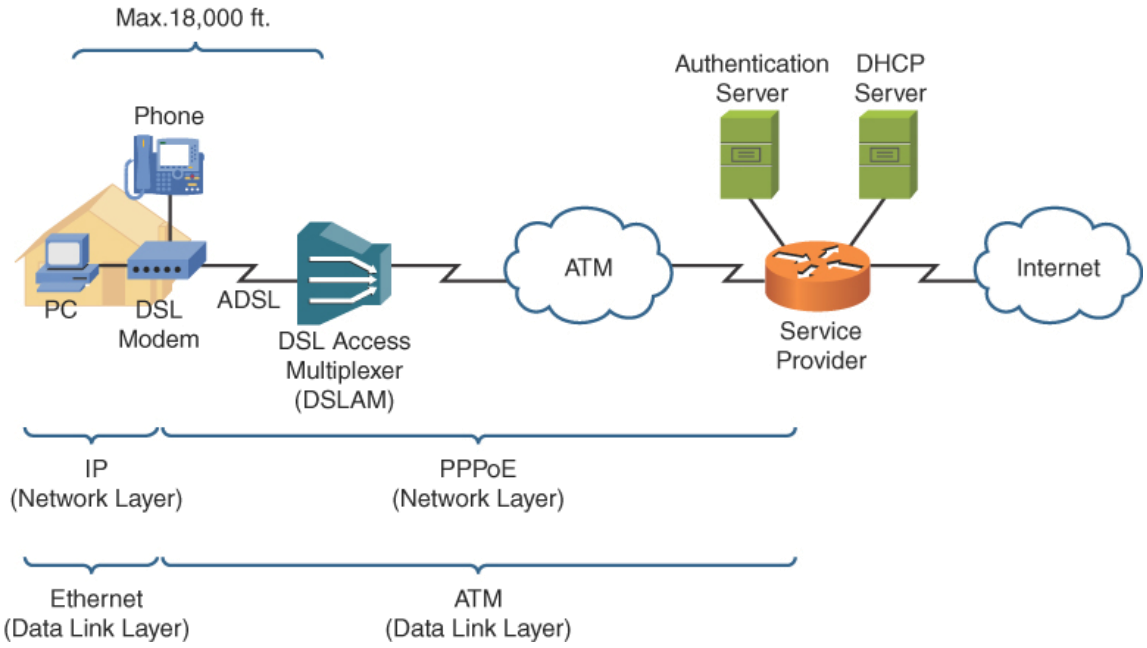
Provider Links
Digital Subscriber Line

- Asymmetric DSL (ADSL)
  - 3.6576 kilometers
    - DSL MODEM-DSLAM
  - downstream /upstream speed is 1.168Mbps



Provider Links
Digital Subscriber Line

- Very High Bit-Rate DSL (VDSL)
  - 1.2192 kilometers
    - DSL MODEM-DSLAM
  - Downstream 52Mbps max speed
  - Upstream 12Mbps max speed



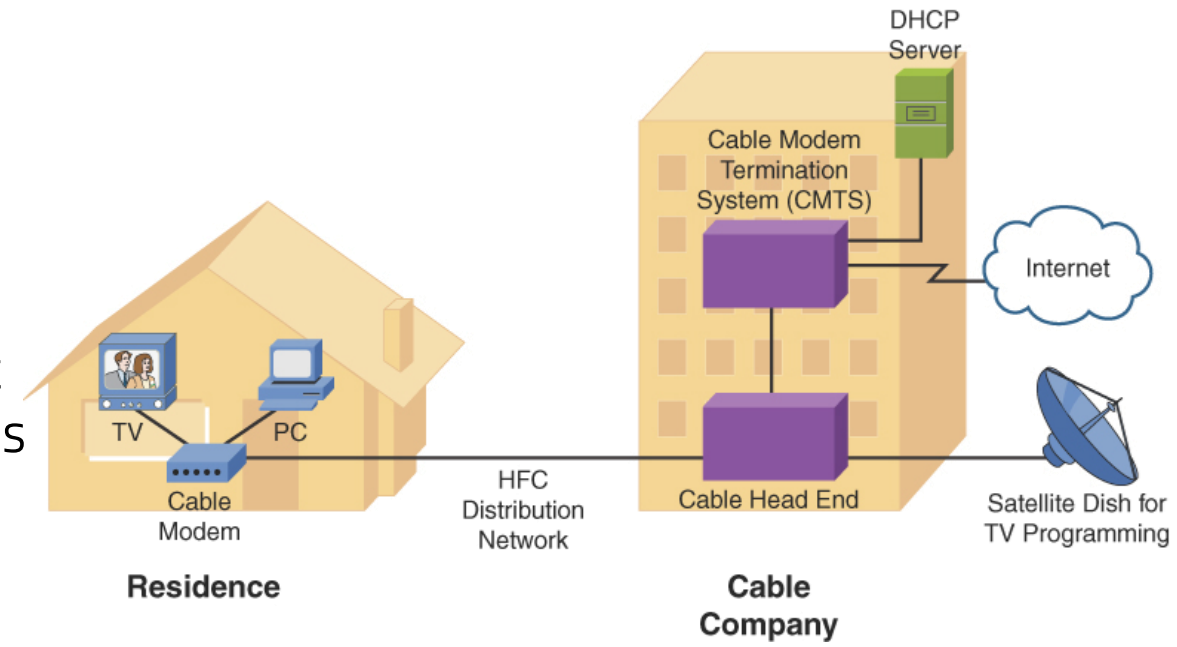
Provider Links
Cable Modem

- Cable television
  - hybrid fiber-coax (HFC)

•Upstream data frequencies: 5MHz to 42MHz

•Downstream data frequencies: 50MHz to 860MHz

•theoretical maximums are 1Gbps upstream and 10Gbps downstream



Provider Links
Leased Line

- Leased line Typically a point-to-point connection interconnecting two sites. All the bandwidth on that dedicated leased line is available to those sites. Often referred to as a dedicated leased line.
- WAN technologies used with dedicated leased lines include digital circuits, such as T1, E1, T3, and E3.

Provider Links
Leased Line

T1 circuit is composed of 24 DS0s, which is called a Digital Signal 1 (DS1). The bandwidth of a T1 circuit is 1.544Mbps:

- Total bandwidth = 1.544Mbps.
- T1 circuits are popular in North America and Japan.

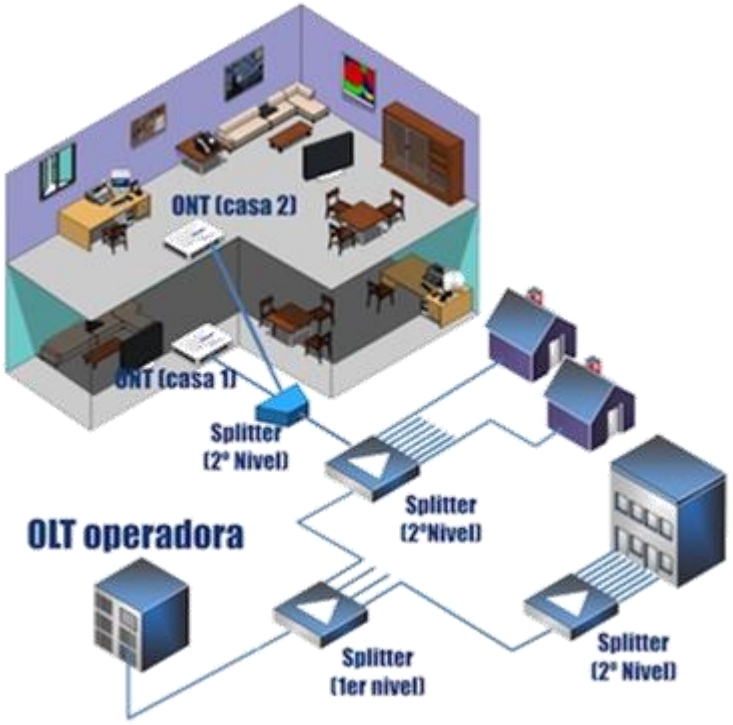
E1 circuit contains 32 channels, in contrast to the 24 channels on a T1 circuit.

- Total bandwidth 2.048Mbps
- E1 circuits are popular outside North America and Japan.

Provider Links
GPON

A GPON (Gigabit Passive Optical Network) is a fiber-optic telecommunications network that uses passive splitters rather than active switches to distribute data, voice, and video signals to multiple users. GPON is a type of PON (Passive Optical Network), which uses fiber-optic cables to transmit data over long distances.

- single fiber-optic cable is used to connect a central office (CO)
- downstream capacity of up to 2.5 Gbps and an upstream capacity of up to 1.25 Gbps, which is shared among multiple users.



Summary

1. Defining a Network
2. Network Types and Characteristics
3. Networks Defined Based on Resource Location
4. Networks Defined by Topology
5. Virtual Network Concepts
6. Provider Links

Bibliografia

- SEQUEIRA, Anthony. *CompTIA Network+ N10-008 Cert Guide*. Pearson IT Certification, 2021.
- ODOM, Wendell. *CCNA 200-301 Official Cert Guide, Volume 2*. Cisco Press, 2019.
- ODOM, W. CCNA 200-301, Volume 1 Official Cert Guide. 2019.