Networking

Networking Fundamentals

1.2.1 Network Topologies

What are the different network topologies and how do they differ?

Overview

The student will be able to explain the characteristics of network topologies and network types.

Grade Level(s)

10, 11, 12

Cyber Connections

- Threats & Vulnerabilities
- Networks & Internet
- Hardware & Software

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

Teacher Notes:

CompTIA N10-008 Network+ Objectives

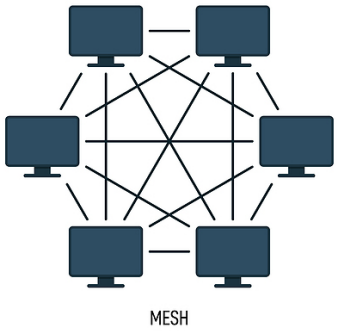
Objective 1.2

- Explain the characteristics of network topologies and network types.
    - Mesh
    - Star/hub-and-spoke
    - Bus
    - Ring
    - Hybrid
    - Network types and characteristics
        - Peer-to-Peer
        - Client-Server
        - Local area network (LAN)
        - Metropolitan area network (MAN)
        - Wide area network (WAN)
        - Wireless local area network (WLAN)
        - Personal area network (PAN)
        - Campus area network (CAN)
        - Storage area network (SAN)
        - Software-defined Wide area network (SDWAN)
        - Multiprotocol label switching (MPLS)
        - Multipoint generic routing encapsulation (mGRE)

Network Topologies

A network topology is a map of a physical network. These maps contain all the devices on the network and how they are connected. These maps are a visual tool to see how data moves on the network.

Mesh

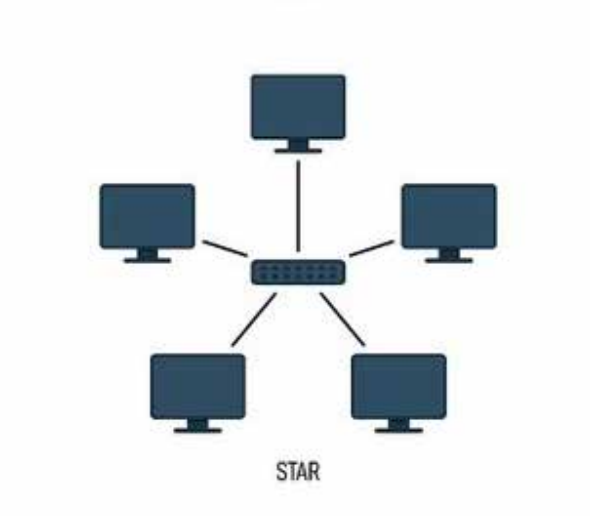


Example of a Mesh Topology

Teacher Notes:

One type of network topology is a ***mesh***. A mesh network is when every device is connected to every other device. This means that there are a lot of connections for each device on the network and would require a lot of cable for each machine to be connected to all the others. A mess network becomes increasingly difficult as more devices are connected to the network.

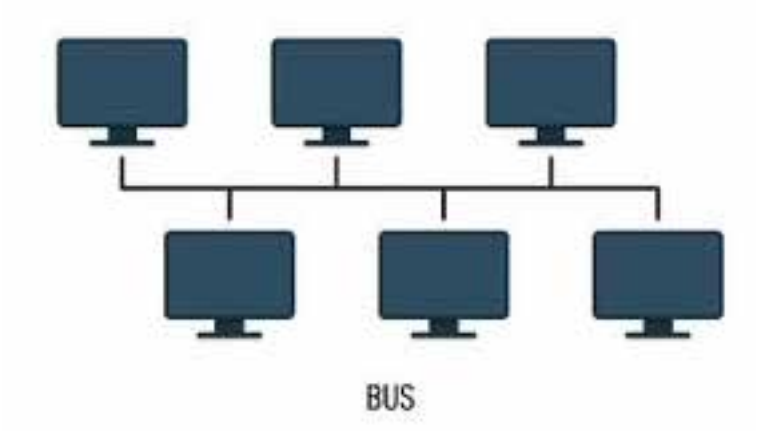
Star/hub-and-spoke



Example of a Star Topology

Another network topology is a ***star*** (also known as ***hub-and-spoke***). A star network is when all the devices are connected to one central device. This central device is typically an access point, hub, switch, etc… The biggest downfall of a star network is when the central device fails, this means all the other devices lose network connectivity (Single point of failure).

Bus

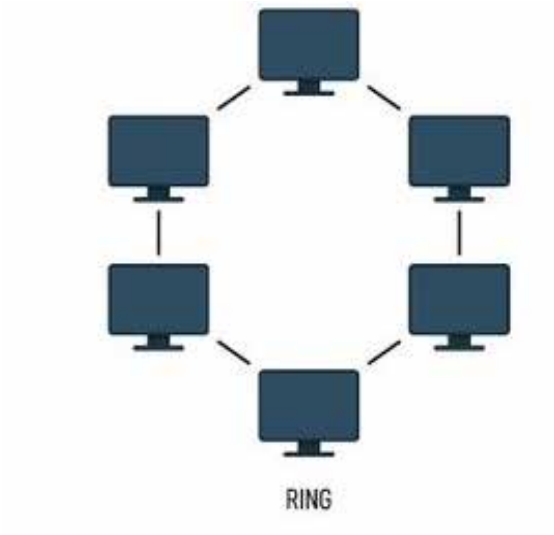


Example of a Bus Topology

Teacher Notes:

Bus topology is when an entire network is connected to one single cable that is the backbone. Obviously, if this central cable fails, the entire network goes down, but requires a lot less cable than other types of topologies. These can be difficult to physically move since the cable is built for the specific space. Since the entire network runs on one cable, adding a lot of devices will slow the network down, thus these are not meant for large networks.

Ring



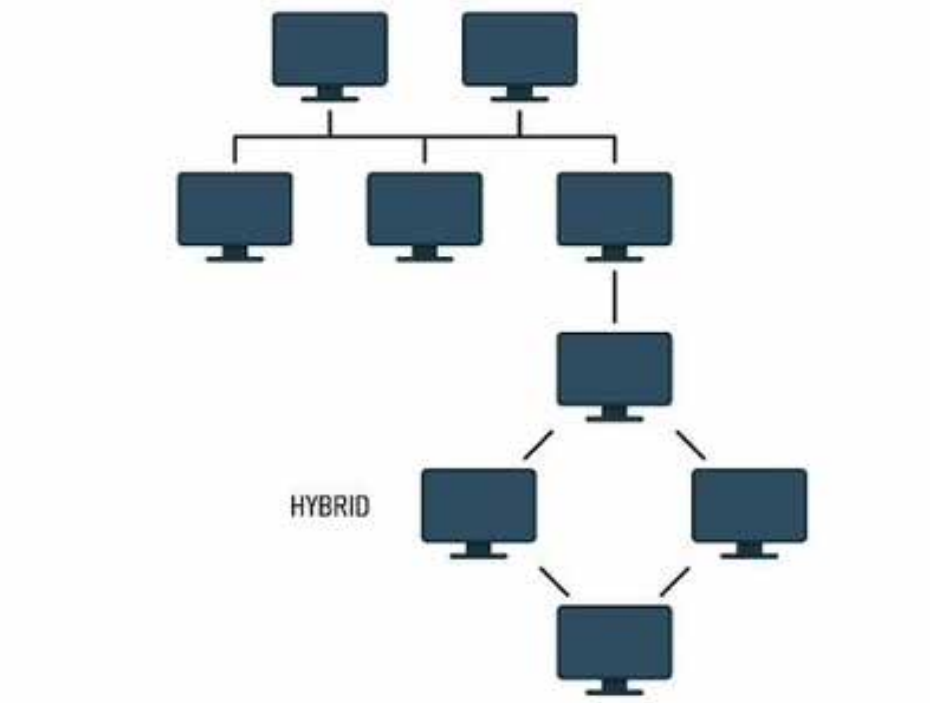
Example of a Ring Topology

From the image, it's easy to see why this topology is called a ***ring***. Here, all the devices are connected in a circle with each device connected to two other devices. A major downfall of this type of network is the ring must be broken to add a new device, thus taking down the entire network to add a device. Ring topology is not very common, especially in LAN networks. Dual rings are used to prevent shutdowns if one of the rings "breaks".

Hybrid

A ***hybrid*** topology is when two or more topologies are combined for the network. In the image, a ring and bus topology have been used to form the network. There are many ways hybrid topologies can look. Hybrid topologies can become difficult to design and maintain but can help personalize a network for specific needs.

Teacher Notes:



Example of a Hybrid Topology

Peer-to-Peer and Client-Server Networks

A ***client-server*** network is when a single server controls the network for all the devices while in a ***peer-to-peer***, all the machines are the client and the server. For example, in a client-server, the server controls all the usernames, passwords, and rights for the network while in a peer-to-peer, each machine controls their own usernames, passwords, and rights to their machine.

You can picture a client-server network as a email server, like gmail, where gmail's servers contain all the log-in information for their users as well as what rights each user has. While a peer-to-peer is like using a smart phone, like an iPhone. Each iPhone sets their own username and password for the device and controls what they can or cannot do on that phone.

WANs and LANs and More

Most networks can be placed into one of two categories: LANs or WANs. A ***local area network (LAN)*** covers a small area, with all the computers connected via cables, wireless signals, or a combination of the two. LANs typically cover one building or a small group of nearby buildings. Home and small office networks are usually LANs.

Teacher Notes:

A ***wide area network (WAN)*** covers a large area, typically composed of two or more LANs connected. For example, all the schools in a district may have a unique LAN per school but could be linked together to form a WAN. The abbreviation WLAN is not to be confused with a combination of LAN and WAN, instead it stands for wireless local area network.

A centralized/location specific WAN can be called a ***metropolitan area network (MAN)***. These networks are specific to an area, typically a metropolitan region, where cables can be placed to transfer data quickly between locations within the MAN.

A ***wireless local area network*** is quite common. These are LANs that allow their users to move around while still being connected to the network wirelessly. A lot of family homes have a wireless LAN where people living in the house can move from room to room and still be on the same network wirelessly.

A ***campus area network (CAN)*** is a network usually on a corporation's campus or a school/university campus. Devices can go from one building to another and still be connected to the same campus network. Devices can be physically plugged into the network or connect wirelessly.

A ***personal area network (PAN)*** is a close proximity network that is usually specific to a certain room. An example could be someone's office where they have their computer connected to their printer and a speaker located in the room. Conference rooms might have a PAN where users can connect to a speaker, microphone, projector, or anything else in the room.

A ***storage area network (SAN)*** is designed to be used with large storage centers for data. These networks contain huge servers hosting data and it is set-up to transfer data between these servers efficiently. Typically, these are not connected with other LANs and WANs.

A completely virtual network is a ***software-defined wide area network (SD WAN or SDWAN).*** This network uses software to connect any/all devices and control their connectivity. Some popular services that host SD WAN networks are Amazon Web Services (AWS) and Microsoft Azure. Here, everything can be hosted in the cloud, thus all connections, machines, etc… are all software-based/virtual.

Teacher Notes:

MPLS and mGRE

Multiprotocol Label Switching (MPLS) is a very popular WAN protocol. Here, when data is sent, it contains label information that is read and then re-routed to a destination based off this information. Instead of a wire leading the information somewhere, the labels are read and the data is transferred. Imagine a school's network, if a teacher wants to send a message to another teacher's computer, they don't have to have a network cable between their two computers, instead the message is sent, the labels tell the MPLS network what teacher to send the message, and then it routes the message to that machine. This becomes more powerful whenever the high school teacher sends a message to an elementary teacher in a different building. The MPLS will route the message not only to the elementary building but also to that teacher.

Multipoint generic routing encapsulation (mGRE) is when a network will create VPNs between devices when they are communicating. A VPN between two corporate offices will be created when they are communicating then the VPN connection will be taken down after completion. While secure, this does end up creating and terminating a lot of VPN connections.