LESSON 1

98-366 Networking Fundamentals

1.1 Understand the Concepts of the Internet, Intranet, and Extranet

1.2 Understand the Local Area Network (LAN)

1.3 Understand VLANs, Wired LANs, and Wireless LANs

1.4 Understand the Wide Area Network (WAN)

1.5 Understand Wide Area Network Connections

1.6 Understand Wireless Network Connections and Security

1.7 Understand Network Topologies and Access Methods

MTA Network Fundamentals 1 Test

LESSON 1.1

98-366 Networking Fundamentals

Understand the Concepts of the Internet, Intranet, and Extranet

Lesson Overview

In this lesson, you will learn about:

- The Internet
- Intranets
- Extranets
- VPN
- Security Zones
- Firewalls

- In 1962 ARPA opened a computer research program and appointed an MIT scientist named John Licklider to lead it. He had just published his first memorandum on the "Galactic Network" concept ... a futuristic vision where computers would be networked together and would be accessible to everyone.
- In October 1969, Internet messaging programs (IMPs) were installed in computers at both UCLA and Stanford. UCLA students would 'login' to Stanford's computer, access its databases and try to send data.

- The experiment was successful and the fledgling network had come into being
- By December 1969 ARPANET comprised four host computers with the addition of research centers in Santa Barbara and Utah
- This was the beginning of the Internet

- Access to the Internet was now available and it was hypertext document servers and Mosaic, the graphical browser, that became the killer application that made the Internet popular and useful to the general public

- This worldwide computer network allows people to communicate and exchange information

- The Internet is not owned by any particular company or person

Intranet

- A private network based on Internet protocols such as TCP/IP but designed for information management within a company or organization
- One of the key advantages of an intranet is the broad availability and use of software applications unique to the needs of a corporation
- It is also a computer network and includes some of the same technologies as the Internet

- Intranet uses include providing access to software applications; document distribution; software distribution; access to databases; and training
- An intranet is so named because it looks like a World Wide Web site and is based on the same technologies, yet is strictly internal and confidential to the organization and is not connected to the Internet proper
- Some intranets also offer access to the Internet, but such connections are directed through a firewall that protects the internal network from the external Web

Extranet

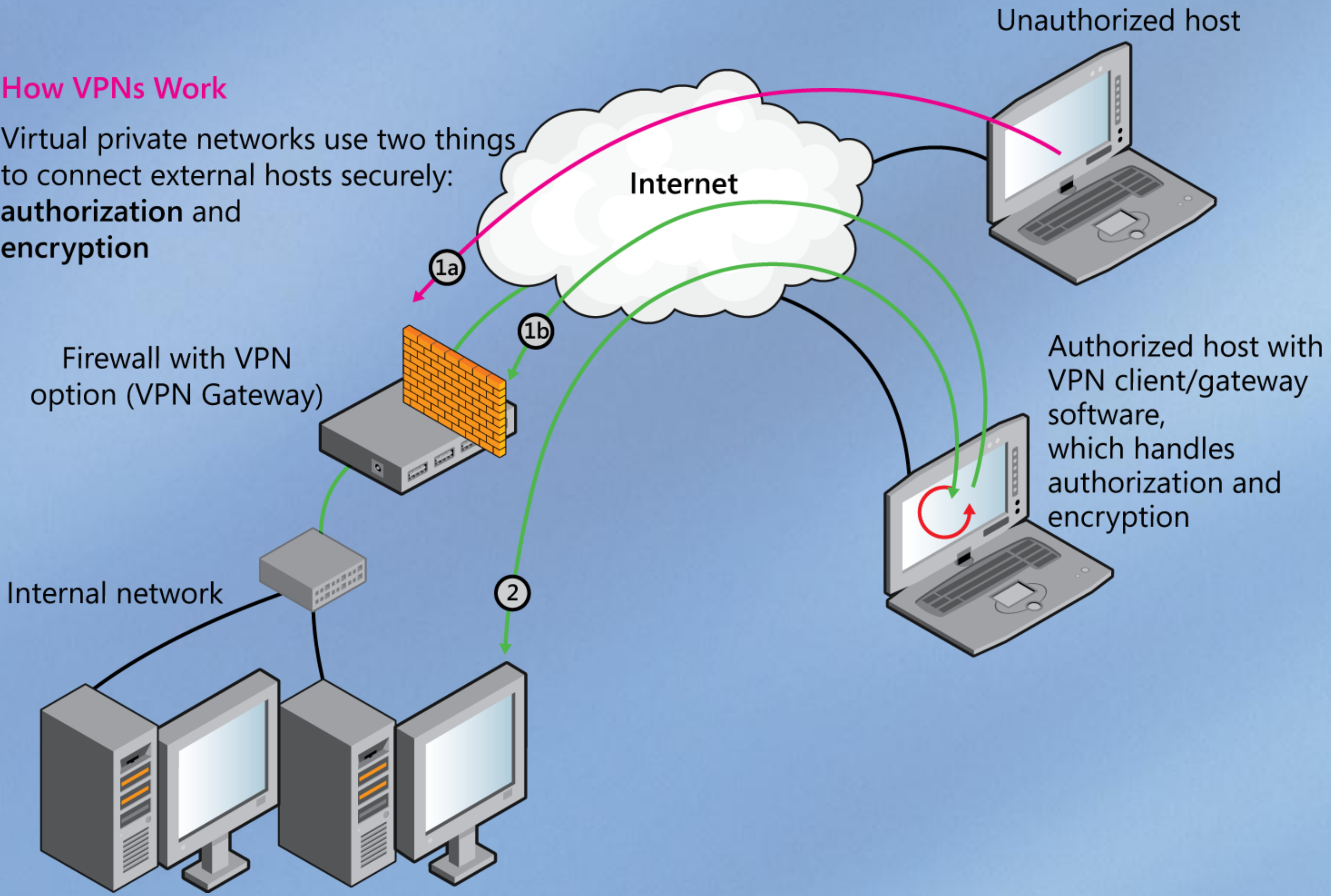
- An extension of some combination of corporate, public, and private intranet using World Wide Web technology to facilitate communication with the corporation’s suppliers, customers, and associates
- An extranet allows customers, suppliers, and business partners to gain limited access to a company’s intranet in order to enhance the speed and efficiency of their business relationship

VPN

- Virtual private network are *nodes* (nodes are a connection point, either a redistribution point or a communication endpoint (some terminal equipment) on a public network
- They communicate among themselves using encryption so that their messages are safe from being intercepted by unauthorized users
- VPNs operate as if the nodes were connected by private lines. An example would be teachers at home needing limited access to the school district’s intranet would be given VPN software for their personal laptop

LESSON 1.1

98-366 Networking Fundamentals



How VPNs Work

Virtual private networks use two things to connect external hosts securely: **authorization** and **encryption**

Unauthorized host
Internet
1a
1b
2
Firewall with VPN option (VPN Gateway)
Internal network
Authorized host with VPN client/gateway software, which handles authorization and encryption

Security Zone

- Business/organization's need for physical and logical boundaries for accessing, controlling, and securing information throughout an organization's network
- The security zone contains hidden settings for how Microsoft Windows and Internet Explorer manage unsigned controls
- Security changes daily. A must to keep aware of the updates. Check the webcasts where leading security and privacy experts in field discuss the issues.
- Microsoft has webcasts covering Security Bulletins, Security Development Lifecycle, Security Intelligence Report, Security Tools, and more

Firewall

- A computer system or network firewall is designed to permit authorized communications while blocking unauthorized access
- The device is configured to permit or deny computer applications based upon a set of rules and other criteria
- Firewalls are technological barriers designed to prevent unauthorized or unwanted communications between computer networks or hosts

Complete Student Activity 1.1

LESSON 1.2

98-366 Networking Fundamentals

Understand the Local Area Networks (LANs)

Lesson Overview

In this lesson, you will learn about:

- LANs
- Perimeter networks
- Addressing
- Local loopback IPs
- An Internet collection

LANs - Local Area Networks

- Computer networks ranging in size from two computers in a home to a few computers in a single office to hundreds or even thousands of devices spread across several buildings.
- They function to link computers together and provide shared access to printers, file servers, and other services.

LESSON 1.2

98-366 Networking Fundamentals

- A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network.
- LANs commonly include PCs and shared resources such as laser printers and large hard disks.
- The devices on a LAN are known as nodes (individual pieces of equipment.)
  - Nodes are connected by wireless and by cables and through which messages are transmitted

- LANs in turn may be plugged into larger networks, such as larger LANs or wide area networks (WANs), connecting many computers within an organization to each other and/or to the Internet.
- The physical media that connect devices, interfaces on the individual devices that connect to the media, protocols that transmit data across the network, and software that negotiates, interprets, and administers the network and its services are all a part of the LAN.

Perimeter Networks

- A perimeter network is a specialized network. Usually a physical subnet outside of the main firewall allowing a business to expose their services to the Internet.

Addresses

- A unique identifier is assigned to each node on a network.
- A computing address defines a range of discrete addresses:
  - each of which may correspond to a physical or virtual memory register
  - a network host
  - peripheral device, disk sector, or other physical entity.
- Just as people have addresses, computer memory and networks have addresses.

Reserved address ranges for local use

- Address ranges are reserved by IANA for private intranets, and not routable to the Internet.
  - Class A: 10.0.0.0 – 10.255.255.255
  - Class B: 172.16.0.0 – 172.31.255.255
  - Class C: 192.168.0.0 – 192.168.255.255

The Internet Assigned Numbers Authority (IANA)

- Allocates ranges of numbers to various registries in order to enable them to each manage their particular address space.

Local Loopback IPs

- 127.0.0.1 is the loopback address in IP
- Loopback is a test mechanism of network adapters. Messages sent to 127.0.0.1 do not get delivered to the network.
- Instead, the adapter intercepts all loopback messages and returns them to the sending application.
- IP applications often use this feature to test the behavior of their network interface.

An Internet Connection Sharing

- ICS is a collection of technologies that work together to enable multiple devices on a private network to share a single Internet connection.
- Microsoft uses the class C reserved IP range for implementing a SOHO (small office/home office) network—where one computer shares its Internet connection with other computers—similar to Microsoft's printer sharing noted in the video.

Complete Student Activity 1.2

LESSON 1.3

98-366 Networking Fundamentals

Understand VLANs, Wired LANs, and Wireless LANs

Lesson Overview

In this lesson, you will review:

- Wired local area networks
- Wireless local area networks
- Virtual local area networks (VLANs)

LAN

- A local area network (LAN) is a single broadcast domain. This means the broadcast will be received by every other user on the LAN if a user broadcasts information on his/her LAN. Broadcasts are prevented from leaving a LAN by using a router.

Wired LAN

- An electronic circuit or hardware grouping in which the configuration is determined by the physical interconnection of the components

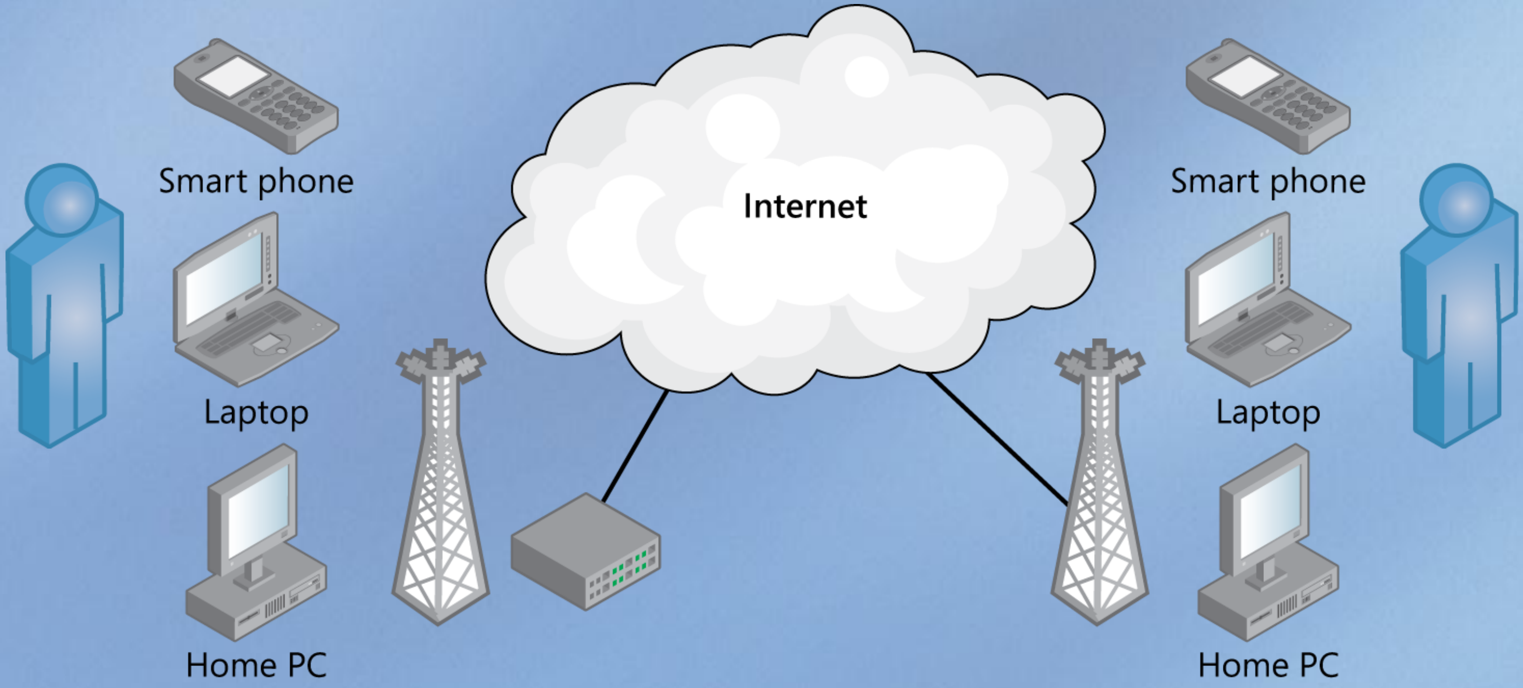
Wireless LAN

- Communications that take place without the use of interconnecting wires or cables, such as by radio, microwave, or infrared light
- Wireless networks can be installed:
  - Peer-to-peer “Ad hoc” mode—wireless devices can communicate with each other
  - "Infrastructure" mode—allows wireless devices to communicate with a central node that can communicate with wired nodes on that LAN

LESSON 1.3

98-366 Networking Fundamentals

Sample example of a wireless LAN design:



Wired LANs: Advantages

Most wired LANs are built with inexpensive hardware:

1. Network adapter

2. Ethernet cables

3. Hubs

Advantages

- Wired LANs provide superior speed and performance

Disadvantages

- Difficult to run cables under the floor or through walls especially when computers sit in different rooms
- Require central devices like hubs or routers to accommodate more computers, which can be expensive
- Generally it costs less than wireless equipment for the equivalent wired Ethernet products

Wireless LANS: Advantages

- Easy access to the Internet in public places
- Less expensive to install and maintain
- Alleviates the need to run wiring through buildings

Disadvantages

- The data transfer rate will decrease as computers are added
- Lower wireless bandwidth means video streaming will be slow
- Security is more difficult to guarantee and requires configuration

Application of LANs

- Home and small business computer networks can be built using either wired or wireless technology
- Large companies are trying to move toward wireless but there are more challenges, especially with security
- Wired Ethernet has been the traditional choice in homes, but Wi-Fi wireless technologies are quickly replacing wired LANs

VLAN

- A virtual LAN, known as a VLAN, is a group of hosts with a common set of requirements that communicate regardless of their physical location
- Sometimes called a “logical network”
- Has the same attributes as a physical LAN, but allows for end stations to be grouped together even if they are not located on the same network switch
- Network reconfiguration can be done through software

- The VLAN controller can change or add workstations and manage load balancing and bandwidth allocation more easily than with a physical picture of the LAN
- Network management software keeps track of relating the virtual picture of the local area network with the actual physical picture

LESSON 1.3

98-366 Networking Fundamentals

Complete Student Activity 1.3

LESSON 1.4

98-366 Networking Fundamentals

Understand Wide Area Networks (WANs)

Lesson Overview

In this lesson, you will review:

- Dial-up
- Integrated services digital networks (ISDN)
- Leased lines
- Virtual private networks (VPN)
- Wide area networks (WAN)

Dial-up Connections

- A connection that uses the public switched telephone networks rather than a dedicated circuit or some other type of private network.
- This is often referred to as plain old telephone service/public switched telephone service (POTS/PSTN).
- Remote server access provides two different types of remote access connectivity:
  - Dial-up remote access
  - Virtual private network (VPN) remote access

- With dial-up remote access, a remote access client uses the telecommunications infrastructure to create a temporary physical circuit or a virtual circuit to a port on a remote access server.
- After the physical or virtual circuit is created, the rest of the connection parameters can be negotiated.

ISDN - Integrated Services Digital Network

- A high-speed digital communications network evolving from existing telephone services.
- Designed to replace the current telephone network
- An ISDN communication channel carries voice, circuit, or packet conversations. The B channel is the fundamental component of ISDN interfaces. It carries 64,000 bits per second in either direction.
- The most common kind of ISDN interface available in the United States is BRI, which contains two B channels, each with 64-kbps capacity, and a single D channel (16-kbps) that is used for signaling and call progress messages.

Leased Lines

- A communications channel that permanently connects two or more locations.
- Leased lines are private or dedicated lines, rather than public ones. Also called *dedicated connection* and *private line.*
- A leased line is a dedicated telephone line rented from the phone company. It provides a 24 hour dedicated connection between two points.
- Leased lines can be almost any speed but are typically 2 Mbps. Higher speed lines are more expensive.

VPN - Virtual Private Network

- Computer devices (nodes) on a public network that communicate among themselves using encryption technology so that their messages are as safe from being intercepted and understood by unauthorized users as if the nodes were connected by private lines.
- VPN client uses an IP (Internet protocol) internetwork to create a virtual point-to-point connection with a remote access server acting as the VPN server.
- A server-based computer can be a remote-access server so that other users can connect to it by using VPN, and then access shared files on your local drives or on your network.

Basic VPN Requirements

- User Permission. Enable a user to access the VPN
- IP Configuration. The VPN server should have a static IP address and assign the arrange of IP addresses to VPN clients.
- The VPN server must also be configured with DNS (Domain Name System) and WINS (Windows Internet Name Service) server addresses to assign to the VPN client during the connection
- Data Encryption. Data carried on the public network should be rendered unreadable to unauthorized clients on the network

Basic VPN Requirements (continued)

- The TCP/IP (transmission control protocol/Internet protocol) is a common protocol used in public networks
- Firewall Ports. VPN server behind the firewall requires port implementation
- Interface(s) for VPN server. If using a router, only one NIC (network interface controller) is needed. If the network doesn't have a router or the VPN is also a gateway, the computer must have at least two interfaces, one connecting to the Internet and another connecting to the LAN.
- One interface for VPN client. The interface can be a dial-in modem, or a dedicated connection to the Internet

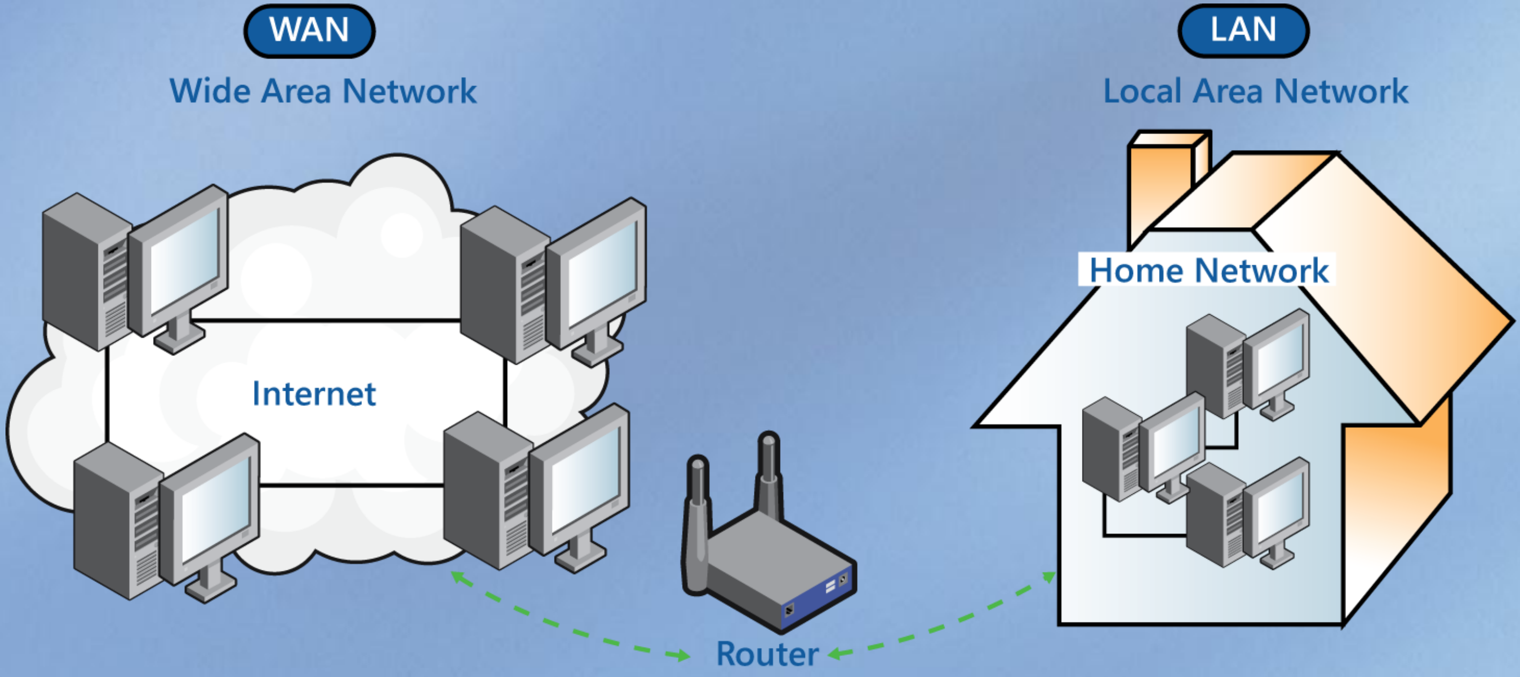
WAN - Wide Area Network

- Geographically widespread network
- Relies on communications capabilities to link the various network segments
- Can consist of a number of linked LANs (local area networks) or it can be one large network
- Used to connect LANs and other types of networks together, so that users and computers in one location can communicate with users and computers in other locations

LESSON 1.4

98-366 Networking Fundamentals

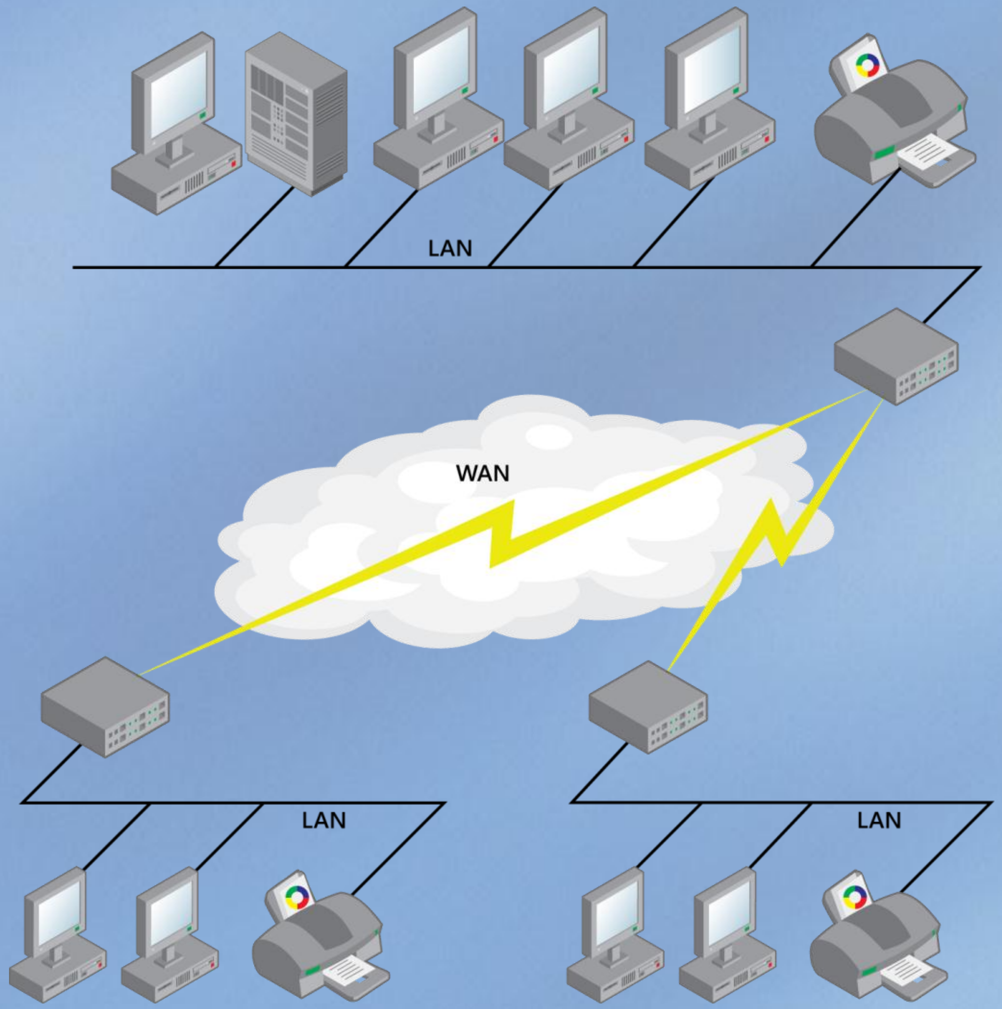
LAN to a Wide Area Network



A router connects your personal LAN to the Internet (WAN).

LESSON 1.4

98-366 Networking Fundamentals



LESSON 1.4

98-366 Networking Fundamentals

Complete Student Activity 1.4

LESSON 1.5

98-366 Networking Fundamentals

Understanding Wide Area Networks Connections

Lesson Overview

In this lesson, you will learn about:

- T1
- T3
- E1
- E3
- DSL
- Cable and its characteristics (speed, availability)

T1

- A high-speed communications line that can handle digital communications and Internet access at the rate 1.544 Mbps (megabits per second).
- This high-bandwidth telephone line can also transmit text and images.
- Speed is attained through multiplexing 24 separate 64 Kbps channels into a single data stream.
- Commonly used by larger organizations for Internet connectivity.

T3

- A T-carrier that can handle 44.736 Mbps (megabits per second) or 672 voice channels.

E1

- A 2.048 Mbps point-to-point dedicated, digital circuit provided by the telephone companies in Europe.
- The European counterpart of the North American T1 line.
- E1 and T1 lines can be interconnected for international use.
- Uses two wire pairs (one for transmit, one for receive) and time division multiplexing (TDM) to interleave 32 64-Kbps voice or data channels.

E3

- A carrier service with capacity for 34.368 Mbps
- The E3 lines is the European counterpart to the US T3
- Europe has a counterpart for every T-carrier leased line capability
- A speed capacity of 34.368 Mbps
  - Interesting since E1 is faster than a T1 and E2 is faster than a T2 but E3 is slower than a T3
- E2 through E5 lines provide multiple E1 channels

DSL - Digital Subscriber Line

- Provides high-speed transmissions over standard copper telephone wiring
- The data throughput of consumer DSL services ranges from 384 Kbps to 20 Mbps in the direction to the customer
    - Depends upon technology, line conditions, and service-level.
- The data throughput in the reverse direction—from customer to the service provider—is lower
    - Asymmetric digital subscriber line (ADSL) is the most common DSL service provided but still with limited availability
    - Symmetric digital subscriber line (SDSL) provides equal speed in both directions

Cable Internet Access through CATV

- Has become a viable alternative and many cable companies are offering both a home and a business-class connection.

LESSON 1.5

98-366 Networking Fundamentals

Complete Student Activity 1.5

LESSON 1.6

98-366 Networking Fundamentals

Understand Wireless Networking Connections & Security

Lesson Overview

In this lesson, you will learn about:

Wireless networking

- Wireless networking standards and their characteristics
- 802.11a, b, g, n including different GHz ranges
- Types of network security
  - WPA
  - WEP
  - 802.1X
- Point-to-point (P2P) wireless
- Wireless bridging
- Gigahertz

Wireless Telecommunications

- Computer networks created without wires such as a local area network (LAN)
- The telecommunications network employ interconnections between nodes implemented without the use of wires
- Wireless telecommunications networks are accomplished with some type of remote information transmission system

Wireless Telecommunications (continued)

- This implementation takes place at the physical level or "layer" of the network where the waves are like radio waves.

- Waveform refers to the shape and form of a carrier signal such as a radio wave. A wave is a disturbance that travels through space and time moving in a solid, liquid, or gaseous medium.

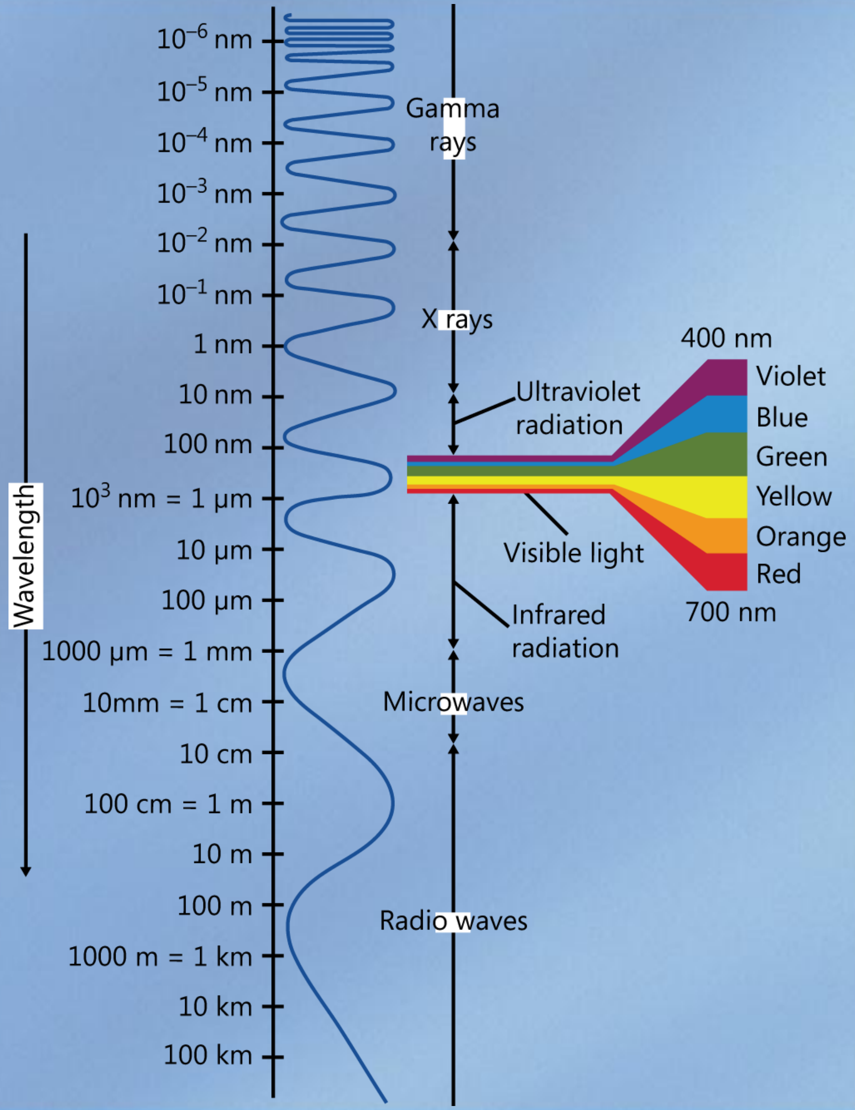
- This carrier signal uses the same basic protocol as a modulating signal.

Electromagnetic Waves

- The wave, or "disturbance," is invisible and is called the force field.
- Without these charged particles, there can be no electric force fields and thus no electromagnetic waves.
- Examples include light, microwaves, X-rays, and TV and radio transmissions are all kinds of electromagnetic waves.
- Negative electrons and positive protons charges cause each other to move.
- Positive charge exerts an attractive force on electrons—an electric force.
- The velocity makes no difference, the pull or force depends only upon where you put it.
- Electronic devices make use of the range of the electromagnetic spectrum.

Wireless

- Describes communications in which electromagnetic waves or RF carry a signal over the entire communication path.
- The frequencies that are available for use for communication are a public resource and are regulated by the Federal Communications Commission in the U.S.



Electronic Modulation

- The process of varying one or more properties of a high-frequency periodic waveform.
- In wireless we first take a signal, like a telephone conversation, and then impress it on a constant radio wave called a carrier.
- It modulates a constant frequency in the radio range, which we can't hear.
- Modulation makes voice band and radio band frequencies work together.
- Different modulation techniques, such as AM and FM, are different ways to shape or form electromagnetic radio waves.

Electronic Modulation (continued)

- Wireless network technologies are used in phones, laptop computers, automobiles, and public transportation.
- High-speed wireless Internet connection services designed to be used from arbitrary locations refers to "mobile broadband.”
- Wi-Fi hotspots provides connectivity over a limited radius around fixed wireless access points.
- The data rate of a computer network connection is measured in units of bits per second (bps).
- One Mbps equals one megabit per second.
- Network equipment makers rate their products using related, larger units of *Kbps*, *Mbps*, and *Gbps*.
- Network outages happen due to limits of the service provider coverage area or obstructions from geography, or even inside larger buildings.

Institute of Electrical and Electronics Engineers (IEEE)

- Creates standards to ensure compatibility.
- The IEEE created the 802 project to develop the standards which are used today. There have been many changes and additions.
- IEEE 802 standards define only certain technologies.
- Most important IEEE 802 standards is the 802.11, wireless networks—it defines standards for wireless LAN communication.
- IEEE 802.11 is a set of standards carrying out wireless local area network (WLAN) computer communication in the 2.4, 3.6 and 5 GHz frequency bands.
- The base current version of the standard is IEEE 802.11-2007. They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802).

Popular Protocols Defined by the 802.11

- 802.11-1997 was the first wireless networking standard.
- 802.11b was the first widely accepted one, followed by
- 802.11g and then by 802.11n.
- 802.11n is a new multistreaming modulation technique.
- The 802.11 family includes over-the-air modulation, which means to change or vary.

- 802.11b and 802.11g use the 2.4 GHz ISM band (industrial, scientific and medical), operating in the United States under Part 15 of the US Federal Communications Commission Rules and Regulations.
- Gigahertz is a measure of frequency.
- Frequency (temporal frequency) is the number of occurrences of a repeating event per unit time.
- The duration of one cycle in a repeating event, so the period is the reciprocal of the frequency.
- Because of this choice of frequency band, 802.11b and g equipment may occasionally suffer interference from microwaves , cordless telephones and Bluetooth devices.

- Both 802.11 and Bluetooth control their interference by using spread spectrum modulation.
- Bluetooth uses a frequency hopping signaling method, while 802.11b and 802.11g use the direct sequence spread spectrum signaling and orthogonal frequency division multiplexing methods, respectively.
- 802.11a uses the 5 GHz U-NII (Unlicensed National Information Infrastructure) band, which offers at least 19 non-overlapping channels rather than the 3 offered in the 2.4 GHz ISM frequency band.
- Depending on the environment, channels may have better or worse performance with higher or lower frequencies.

WEP and WPA

- Wireless security protocols widely used by wireless networking devices
- WEP—Wired Equivalent Privacy or Weak Encryption Protocol
  - Designed to provide equivalent level of security as a wired network
- WPA—Wi-Fi Protected Access (WPA and WPA2)
  - A certification program to designate compliance with the security protocol to secure wireless computer networks
  - Implements the majority of the IEEE 802.11i standard
- The Wi-Fi Alliance intended WPA as an intermediate measure to take the place of WEP pending the preparation of 802.11i
- IEEE 802.11 wireless networks are NOT secured by WEP as it is easily broken

Wireless Security

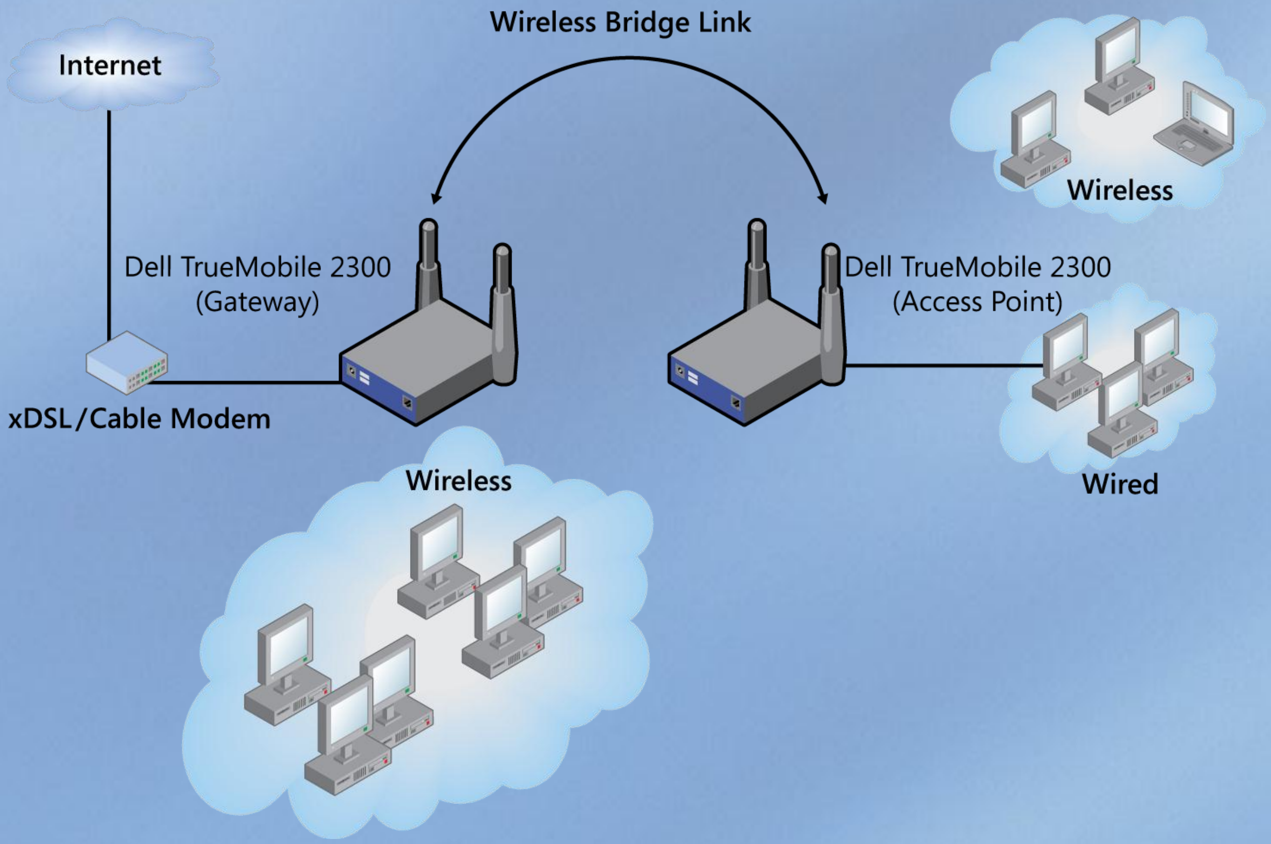
- Wireless network messages are more susceptible to eavesdropping than wired networks.
- A WEP key uses a passphrase – a security code that is produced using this protocol that allows computers to hide the contents of the messages from intruders and exchange coded messages.
- WPA-PSK (Pre-Shared Key) mode provides strong encryption protection without the enterprise authentication server and is the easiest way to deploy WPA to home wireless network using a passphrase.
- WPA uses Temporal Key Integrity Protocol (TKIP) to produce unique encryption keys and automatic rekey each wireless clients from passphrase and network SSID.

LESSON 1.6

98-366 Networking Fundamentals

Wireless Bridging

- A bridge is used to connect two network segments.



Bridging

- A forwarding technique used in packet-switched computer networks.
- Can be done wired or wireless and used only in LANs.
- Bridging depends on flooding and examination of source addresses in received packet headers to locate unknown devices.
- A network bridge connects multiple network segments at the data link layer (Layer 2) of the (OSI) Open System Interconnection model.
- A switch is a bridge with numerous ports. Switch or Layer 2 switch is often used interchangeably with bridge.

Bridging (continued)

- Another form of bridging, source route bridging, was developed for token ring networks.
- The main purpose of wireless bridging is to connect a wired Ethernet network segment to a wireless Ethernet network segment .
- This is most commonly found in a home wireless router that has a built-in multiport switch for wired devices, and a wireless networking WAN connection for DSL or cable for Internet access.

Point-to-Point Protocol (PPP)

- A data link protocol commonly used to establish a direct connection between two networking nodes
- Provides compression, transmission encryption privacy, and connection authentication
- Used over many types of physical networks including serial cable, phone line, trunk line, cellular telephone, specialized radio links, and fiber optic links such as links
- Internet service providers (ISPs) use PPP for customers' dial-up access.
- Internet service providers (ISPs) use two encapsulated forms of PPP to connect Digital Subscriber Line (DSL) Internet service.
    - Point-to-Point Protocol over Ethernet (PPPoE)
    - Point-to-Point Protocol over ATM (PPPoA)

Complete Student Activity 1.6

LESSON 1.7

98-366 Networking Fundamentals

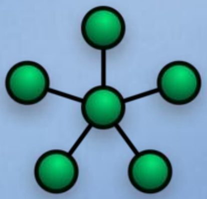
Understand Network Topologies and Access Methods

Lesson Overview

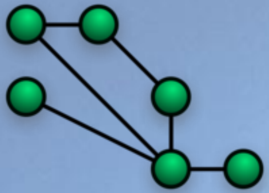
In this lesson, you will learn about:

- Network topologies and access methods

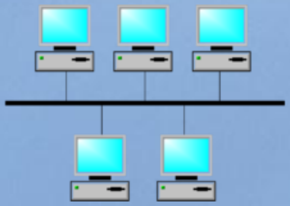
Star



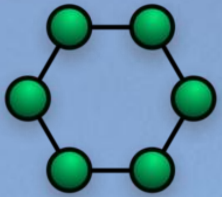
Mesh



Bus



Ring



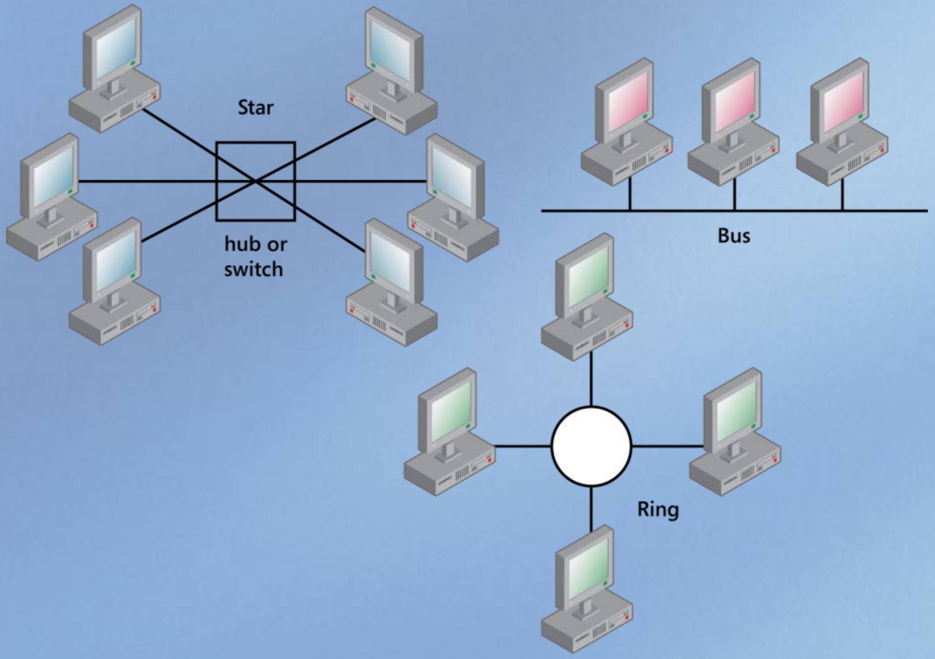
Network Topologies

- The interconnection of the various elements (links, nodes, etc.) of computer equipment
- Network Topologies can be physical or logical
- Topology is the virtual shape or structure of a network, which does not need to correspond to the actual physical design of the devices on the computer network.
- The physical design of a network including the devices, location, and cable installation is known as physical topology.
- How data actually transfer in a network, as opposed to its physical design, is the logical topology, also called signal topology.
- Distances between nodes, transmission rates, physical interconnections, and/or signal types may differ in two networks and yet their topologies may be identical.

LESSON 1.7

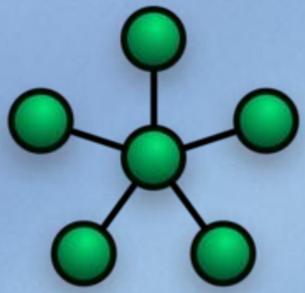
98-366 Networking Fundamentals

- Compare the **logical and physical** topology of the star
- If a hub is used, then the topology is a physical star and a logical bus.
- If switch is used, then the topology is a physical star and a logical star.
- If IBM MAU is used, then the topology is a physical star and a logical ring.



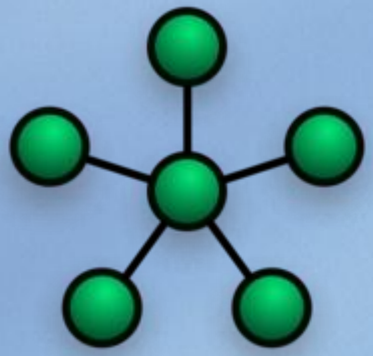
Star Network

- The topology structure of a star network consists of one central switch, hub or computer, which acts as a conduit to transmit messages.
- The hub and leaf nodes, and the transmission lines between them, form a graph with the topology of a star.
- An active **star network** has an active central node that usually has the means to prevent echo-related problems.



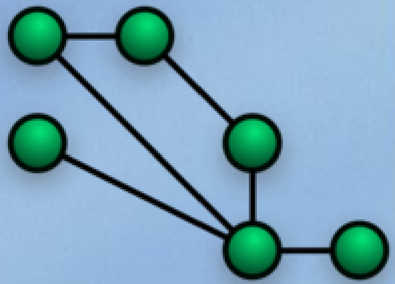
- By connecting all of the systems to a central node, the star topology reduces the chance of network failure.
- The central hub rebroadcasts all transmissions received from any peripheral node to all peripheral nodes on the network when applied to a bus-based network.
- All peripheral nodes may thus communicate with all others by transmitting to, and receiving from, the central node only.
- Isolation of a peripheral node from all others occurs when there is a failure of a transmission, but the rest of the systems will be unaffected.
- Each node (file servers, workstations, and peripherals) is designed to be connected directly to a central network hub, switch, or concentrator.

- Data on a star network passes through the hub, switch, or concentrator before continuing to its destination.
- The functions of the network are controlled and managed by the hub, switch, or concentrator, and it acts as a repeater.
- The twisted pair cable is the most often used although it can be used with coaxial cable or optical fiber cable.



Mesh Networks

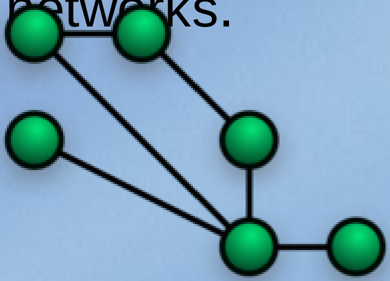
- Each node in the network acts as an independent router.
- A mesh network whose nodes are all connected to each other is a fully connected network.
- The component parts connect to each other via multiple hops.
- Is self-healing and can still operate when one node breaks down or a connection goes bad
- Considered more reliable than other networks
- Mobile ad hoc networks (MANET) must deal with the problems of the mobility of the nodes. Mesh networks do not have this problem but they are closely related with the MANET network.



LESSON 1.7

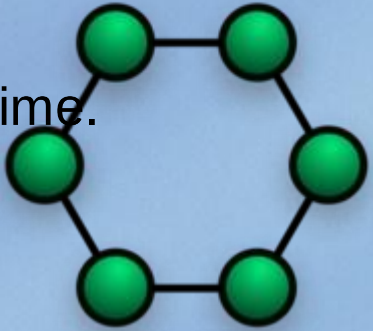
98-366 Networking Fundamentals

- Originally developed for military applications
- Wireless networks are typical of mesh architectures.
- The mesh network can support multiple functions such as client access, backhaul service, and scanning in mobile applications.
- Increased power has enabled the mesh nodes to become more modular.
- One node or device can contain multiple radio cards or modules, allowing the nodes to be customized to handle a unique set of functions and frequency bands.
- Game theory methods that analyze strategies for the allocation of resources and routing of packets have aided mesh networks.

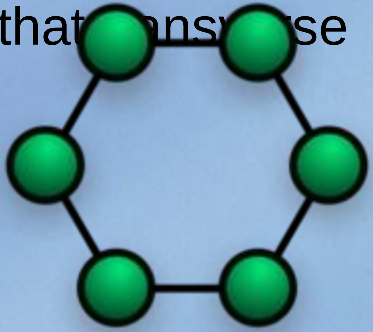


Ring Network

- Data travels from node to node, with each node along the way handling every packet.
- It forms a single continuous pathway for signals through each node.
- May be disrupted by the failure of a single link
- A node failure or cable break might isolate every node attached to the ring.
- Each machine or computer has a unique address that is used for identification purposes.
- Only one machine can transmit on the network at a time.

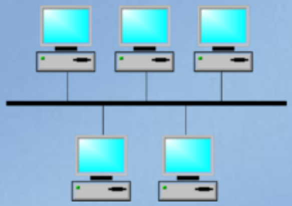


- Even though computers on a home network can be arranged in a circle shape, it does not mean that it presents a ring topology.
- By sending data on a counter clockwise ring FDDI (fiber distributed data interface) networks circumvent a node failure or cable break.
- 802.5 networks, also known as Token Ring networks, avoid the weakness of a ring topology altogether.
  - They actually use a *star* topology at the *physical* layer and a multi-station access unit (MAU) to *imitate* a ring at the *data-link* layer.
- The signal can be boosted or repeated as the computers connected to the ring act to strengthen the signals that transverse the network.



Bus Network

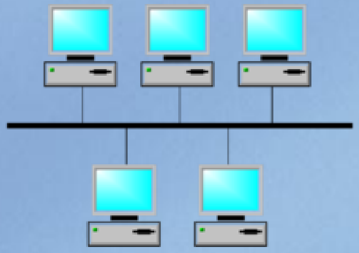
- A shared communications line
- A common backbone to connect all devices that operates and functions as a shared communication medium
- A single cable that devices attach or tap into with an interface connector
- Communicates by sending a broadcast message onto the wire for all other devices to see, but only the intended recipient actually accepts and processes the message.
- Devices on the bus must first determine that no other device is sending a packet on the cable before any device can send a packet.



LESSON 1.7

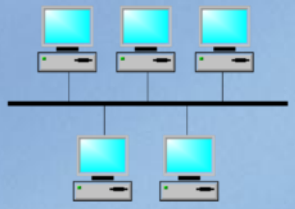
98-366 Networking Fundamentals

- Bus mastering is supported by many bus architectures that enable a device connected to the bus to initiate transactions.
- Devices with Ethernet communicate like they were in chat room, which is called carrier sense multiple access/ collision detection (**CSMA/CD**).
- Two packets are sometimes sent (two cards talk) at the same time.
- The cards arbitrate on their own to decide which one will resend its packet first when this collision occurs.
- All PCs share the data transfer capacity of that bandwidth (wire) if they are on a bus network.



Advantages of a Bus Network

- Easy to implement and extend
- Well-suited for temporary or small networks not requiring high speeds (quick and easy setup)
- Cost effective; only a single cable is used
- Cheaper than other topologies
- Easy identification of cable faults



Disadvantages of Bus Networks

- Limited cable length and number of stations
- Only one packet can remain on the bus during one clock pulse
- If there is a problem with the cable, the entire network breaks down.
- Performance degrades as additional computers are added or with heavy traffic
- Slower data transfer rate than other topologies
- It works best with limited number of nodes

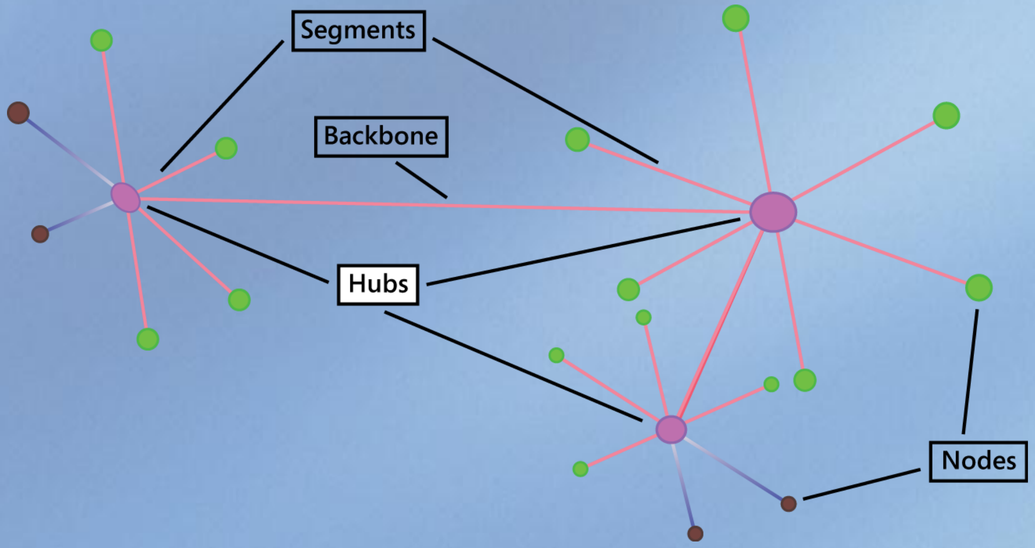
Hybrid Network

- When a combination of two or more topologies are connected
- If two star networks were connected together, they would exhibit a hybrid network topology.
    - A star ring network would be two or more star topologies linked together using a multistation access unit (MAU) as a centralized hub.

LESSON 1.7

98-366 Networking Fundamentals

- Two or more star topologies connected using a bus trunk would be a star-bus network.
- A multi-station access unit (MSAU) connects a group of computers to a token ring local area network.



- **Complete Student Activity 1.7**

Complete Quia Test:

MTA NetFund1 Test