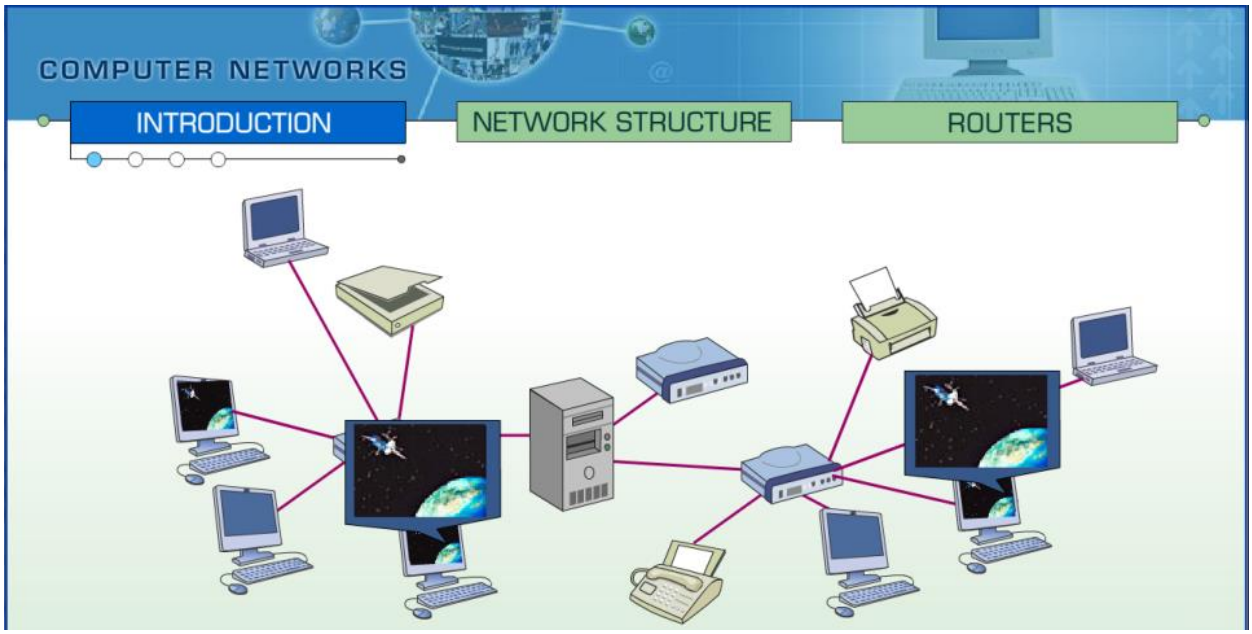
Networking

Zhofrph wr wkh qhwzrunlqj xqlw

It's amazing what you can do with computers, smartphones, iPads, etc. today all while sitting on your bed, at the kitchen table, or even laying out at the pool. Watch the presentation to get a great introduction to computer networks.

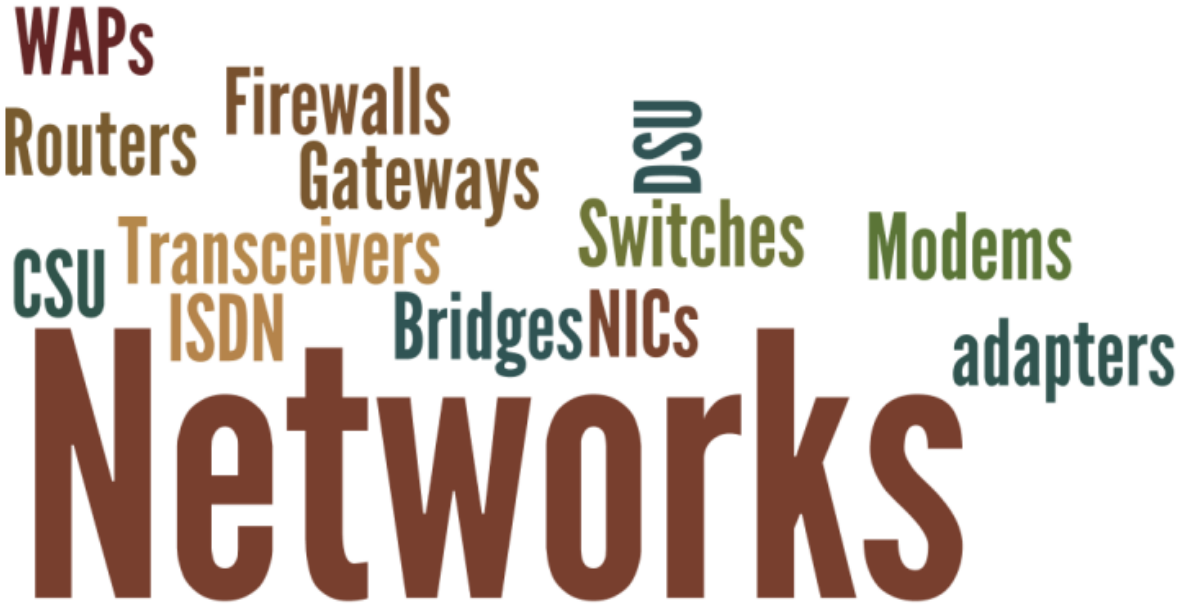


Click on the picture to watch the presentation

A network is a system of computers and peripherals that are linked together. You are taking advantage of the world's largest network right now as you read this website. The Internet consists of billions of computers connected together to form the world's largest wide area network of computers. The purpose of a network is usually to share files, resources, and peripherals such as a printer. You might have a local area network right in your own home. Are you sharing an Internet connection with other computers in your house? How about sharing a printer?

There will be about **fifteen billion** devices connected by 2015, and around forty billion devices by 2020.

Networks enable people to work together while reducing costs. People are able to share networked hardware and software. Productivity is also increased by being able to easily share data. Networks provide access to a wide range of services and specialized peripheral devices. However, there are some disadvantages to networks such as the unavailability of resources when the network malfunctions. Networks are more susceptible to unauthorized access, or hacking, than stand-alone computers and also more susceptible to viruses, worms, Trojan horses and blended threats.



Assignment: Networking Vocabulary

Directions: Define the networking vocabulary listed in the itsLearning assignment. Place your definitions directly in the itsLearning textbox. Do not attach a separate document. Be sure to proofread.

Assignment: Question for Thought

Directions: Visit the Computer History Museum. After reading each year listed, pick four that you found interesting and tell me why. Be sure to include the year and why it was significant. Place your response in the textbox below. Do not attach a separate document and make sure you proofread.

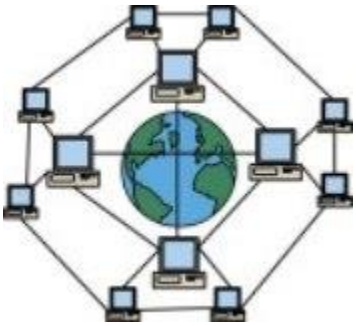
Network Components

A network is made up of **clients** and **servers**. Clients are computers, usually desktop computers with their own local storage and processing power, that request or order information from a server. A client could also be a thin client which is a network computer with no local storage.

Servers are computers that work behind the scenes to provide, or serve, the resources requested by the clients. Servers can be dedicated, providing only one type of resource to its clients, such as printing, or non-dedicated, thus providing different services to clients such as file retrieval, printing and email.

Specialized servers include:

- File Servers
- Print Servers
- Application Servers
- Mail Servers
- Communication Servers
- Directory Services Servers
- Backup Servers



In addition to the clients and servers, networks generally have **shared peripherals** that are connected to a computer and controlled by its microprocessor. There are also **media**, physical pieces used to transport data from one computer to another computer or peripheral on the network, and **data packets**.

Types of Networks

A local area network (LAN) is a network of computers located in a single location, like a home, school, or office building. The computers can share connection with other LANS and with the Internet.

Characters of a LAN include:

- Local area network
- Relatively limited in size
- Computers connected in small areas
    - Same office
- True peer-to-peer
- Can support limited number of nodes

A **Wide Area Network (WAN)** is a network over a large area like a city, a country, or multiple countries. WANS connect multiple LANs together. Generally, WANS utilizes different and much more expensive networking equipment than LANs.

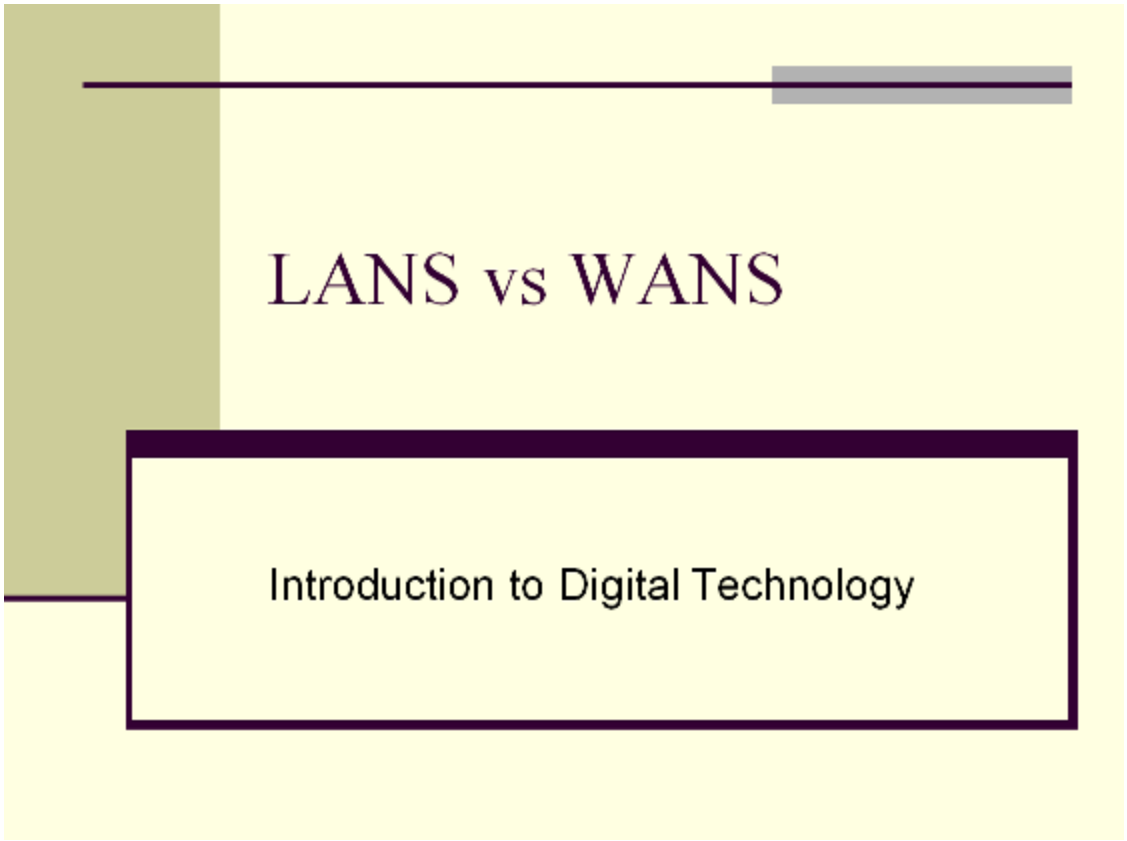
Types of WANs include:

- Campus Area Network – limited geographic area
- Metropolitan Area Network – towns and cities

Do you know the difference between *the* Internet (capital I) and an internet (lowercase i)?

The Internet is the world wide area network that we use for the World Wide Web and an internet is a local area network like in a computer lab.

- Home Area Network – home setups
- Global Area Network – uses satellites to link networks
- Storage Area Network – stores large amounts of data



Click on the picture to watch the presentation

Assignment: LANs vs. WANs worksheet

Directions: Complete the online worksheet in itsLearning.

Networks can be wired or wireless. **Wired networks** are fast, secure, and simple to configure. A wired network uses different wires and cables to connect network devices:

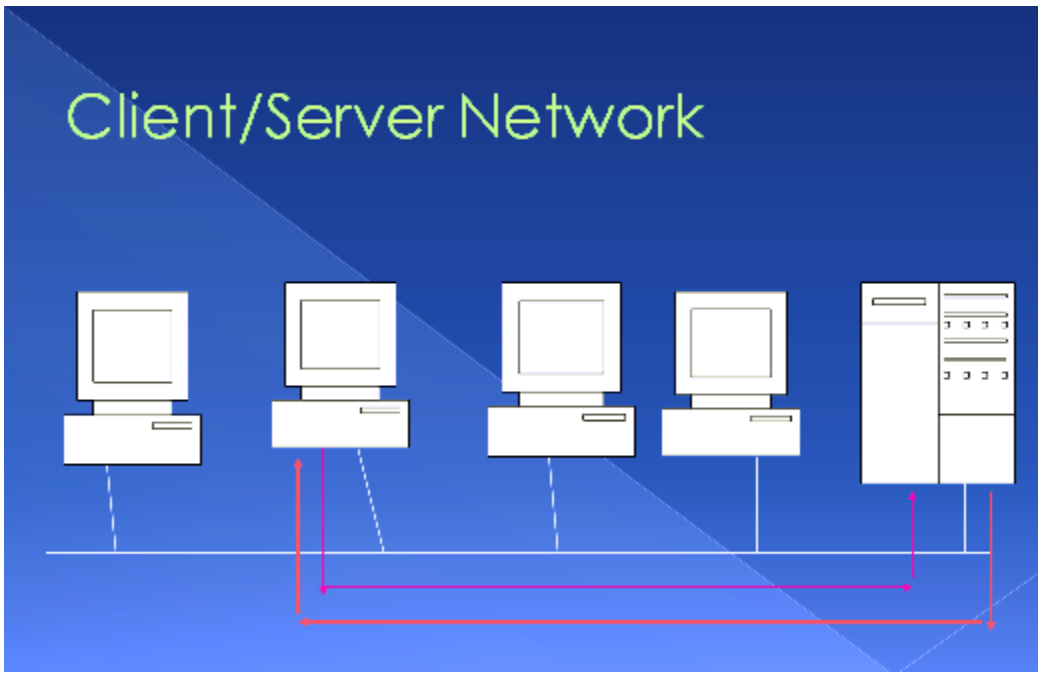
- Ethernet cable - often used to connect computers and plugs into the Ethernet port in the back of the desktop or laptop computer
- Phone or cable TV lines – connect LAN to an Internet service provider (ISP)
- Fiber optic cable – used by much of the Internet to send data quickly over long distances underground

A network is considered **wireless** when data is transmitted from one device to another without cables or wires. Instead of cables or wires, the data is transferred through

satellite waves. Many devices can use Wi-Fi, e.g., personal computers, video-game consoles, smartphones, some digital cameras, tablet computers and digital audio players. These can connect to a network resource such as the Internet via a wireless network access point. Wireless networks tend to be slower than wired networks. Wireless networks also have more security issues compared to wired networks because an intruder does not need a physical connection. An attacker who has gained access to a Wi-Fi network router can initiate a DNS spoofing attack against any other user of the network by forging a response before the queried DNS server has a chance to reply.

Wi-Fi (wireless fidelity) is a common standard technology for guiding home wireless networks and other LANS. Many businesses will use Wi-Fi technology to allow the public an access point to a wireless network. Many restaurants and fast food places will advertise wireless hotspots as a way of attracting customers. **Bluetooth** allows handhelds, cellphones, and other peripherals to communicate over short ranges and uses wireless technology to do so.

Client/Server Networks

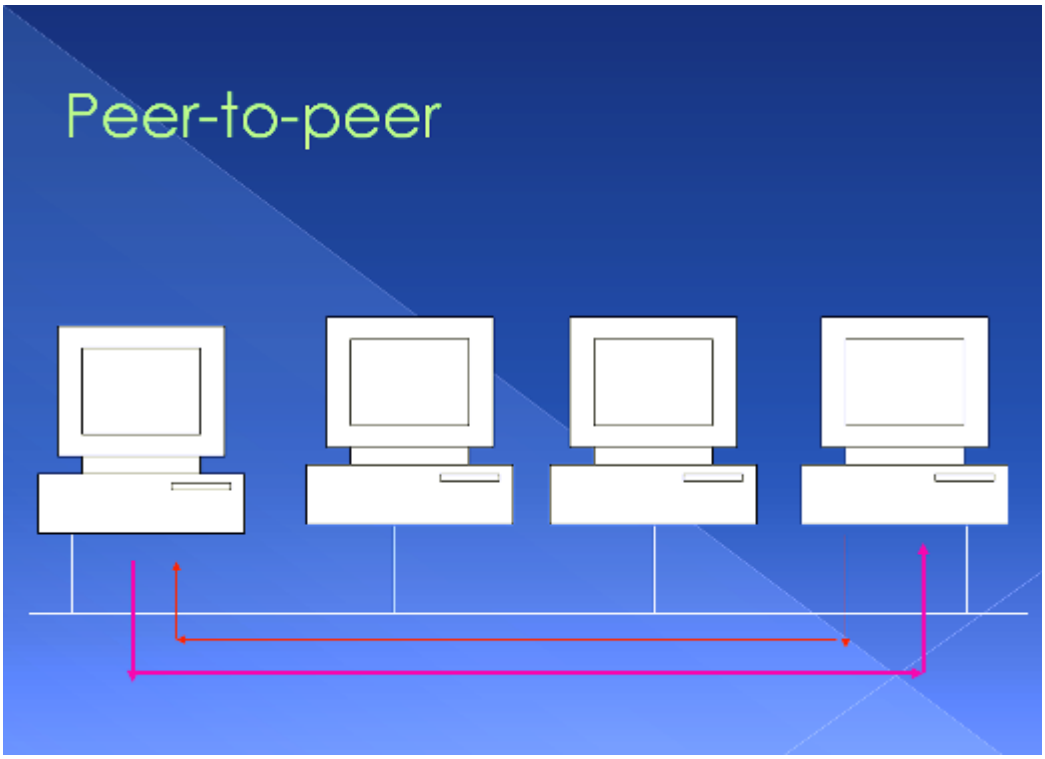


Network devices can function as clients or servers. A **server** is a computer that performs administration or coordination functions within a network. Types of servers include:

- application
- file
- print

A **client** is a regular workstation that performs applications. Your personal computer could operate as both a server and a client in a peer-to-peer network.

Peer-to-Peer Network



A peer-to-peer network is comprised of personal computers, each of which acts as both client and sever, so that each can exchange files directly with every other computer on the network. Each computer can access any of the others, although access can be restricted to those files that a computer's user chooses to make available. A peer-to-peer network is less expensive than client/server networks but less efficient when large amounts of data need to be exchanged.

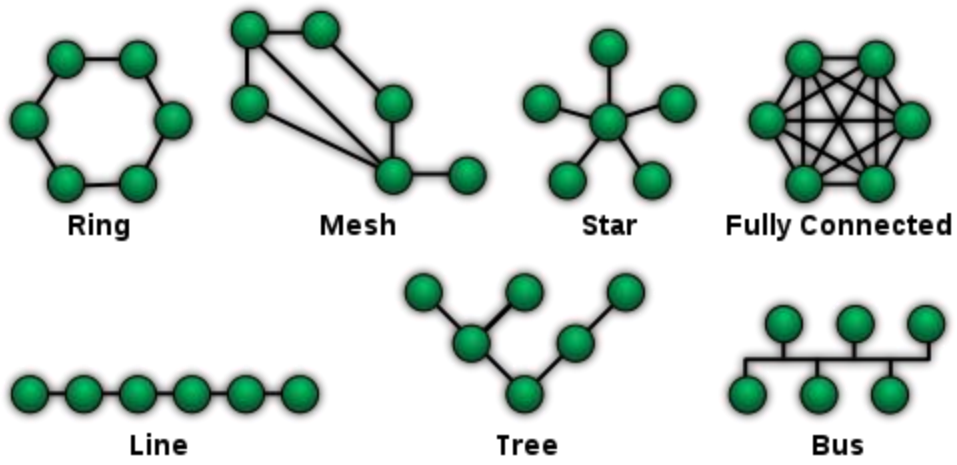
To determine which type, peer-to-peer or client/server, network architecture to set up and utilize, you should start with the type of user and the size of the organization. The peer-to-peer network is utilized in homes and small businesses because it is inexpensive to implement and the user is the administrator. The client/server network is great for large corporations, schools, and hospitals because of the large number of users and workstations it can accommodate but it is more expensive than the peer-to-peer network.

Comparison of ...

	Peer-to-peer	Client/Server
Type of user	Homes and small businesses	Large corporations, schools, and hospitals
Size of organization	Limited number of workstations	Large number of workstations
Administration	User	Central administrator
Security	Individual users	Network administrator
Network traffic	Limited number of users	Large number of users
Cost	Inexpensive to implement	Usually more expensive than peer-to-peer
Scalability	Limited growth	High growth projected

Network Topology

A **network topology** is the physical arrangement of the various elements/devices (links, nodes, etc.) of a computer network.



There are eight basic network topologies:

- Point-to-point
- Bus

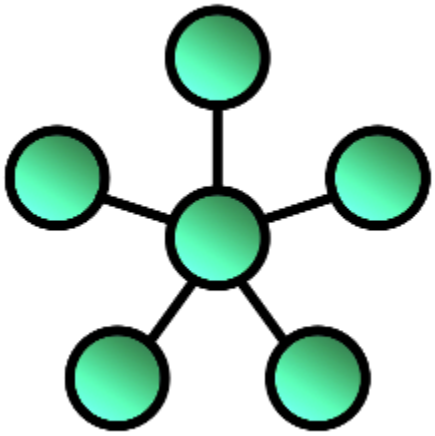
- Star
- Ring or circular
- Mesh
- Tree
- Hybrid
- Daisy chain

The most common network topologies are:

- Star
- Ring
- Bus
- Tree
- Hybrid

A few considerations when choosing a topology are cost, type and length of cable needed, and future growth of the network.

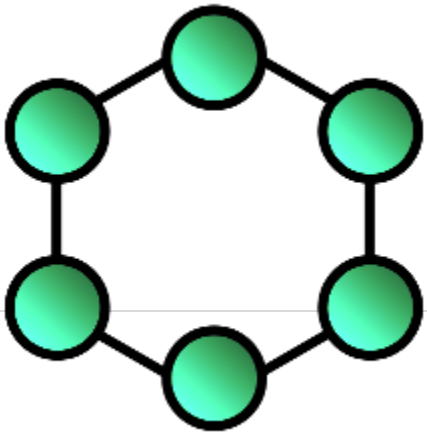
Star Topology



A star topology features a central connection point called a "hub“; that may be a hub, switch or router. It is often used in home networks. It is easy to install and failure of a single cable will only take down one computer's network access and not the entire LAN thus making it easy to detect faults and to remove parts. However, the star topology does require more cable than a linear topology and if the hub fails, the entire network fails.

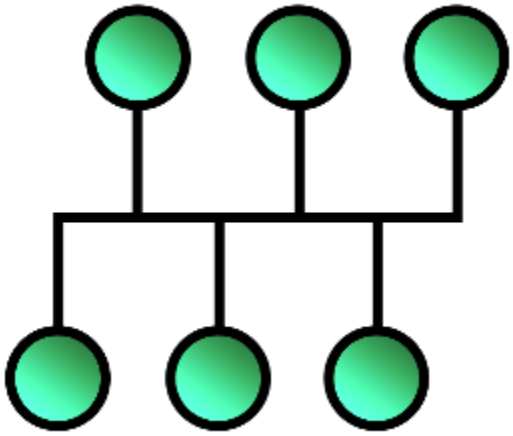
Ring Topology

In a ring topology, every device has exactly *two* neighbors for communication purposes (device on the left and the device on the right). All messages travel through a ring in the same direction (either "clockwise" or "counterclockwise"). A failure in any cable or device breaks the loop and can take down the entire network. Ring topologies can be



found in some office buildings or school campuses.

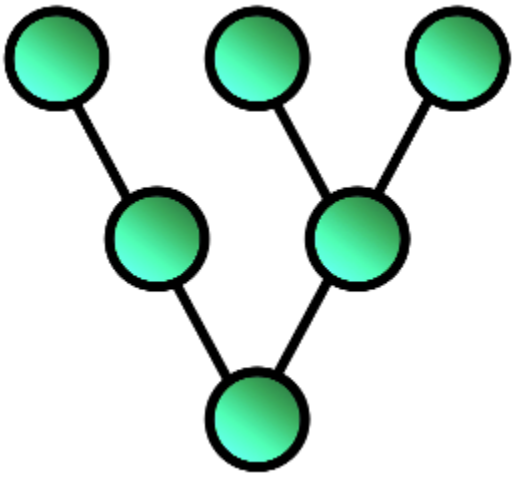
Bus Topology



A bus topology is has a common backbone (a single cable) to connects all devices and devices attach, or tap into, the cable with an interface connector. Devices wanting to communicate with other devices on the network send a broadcast message onto the wire that all other devices see, but only the intended recipient actually accepts and processes the message. A bus topology is easy to connect a computer or peripheral to a linear bus and requires less cable length than a star topology. Disadvantages of a bus topology are that the entire network shuts down if there is a break in the main cable. Terminators are required at both ends of the backbone cable and it is difficult to identify the problem if the entire network shuts down. A bus topology works best in networks with just a few computers.

Tree Topology

A tree topology integrates multiple star topologies together onto a bus topology. In its simplest form, only hub devices connect directly to the tree bus and each hub functions as the "root" of the tree. The tree topology uses point-to-point wiring for individual segments and is supported by several hardware and software vendors. It is easier to expand than either the bus or the star topologies. Overall, the length of each segment is limited by the type of cabling used and if the backbone line breaks, the entire segment comes down. It is more difficult to configure and wire than other types of topologies.



Hybrid Topology

A hybrid topology is a combination of any two or more network topologies. A hybrid topology always accrues when two different basic network topologies are connected. Two of the same topologies, when connected together, may still retain the basic network character, and therefore not be a hybrid network. For example, a tree network connected to a tree network is still a tree network, but two star networks connected together exhibit hybrid network topologies.

Assignment: Network Comparison Chart

Directions: Complete the network comparison chart. Download the template from itsLearning. Do not use the pictures from this presentation. Find others using your research skills and the World Wide Web.

Protocols

A protocol is a set of rules that govern the connection, communication, and data transfer between computers on a network. These rules include guidelines that regulate the following characteristics of a network: access method, allowed physical topologies, types of cabling, and speed of data transfer. There are hundreds of different Internet protocols.

Warriors on the Net

Hypertext Transfer Protocol (HTTP) & Hypertext Transfer Protocol over Secure Socket Layer (HTTPS)

HTTP is a protocol used by the World Wide Web that defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. Most Web sites that you visit will use the HTTP communication protocol. The HTTP protocol built on top of TCP and the three main

HTTP message types are GET, POST, and HEAD.

HTTPS is a combination of normal HTTP interactions, but with a different default TCP port and an additional encryption/authentication layer between the HTTP and TCP. It is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons. It ensures reasonable protection from eavesdroppers and man-in-the-middle attacks. You should make sure that your banking Web site and online transactions Web sites like Amazon are using HTTPS. Look at the URL in the address bar of your browser to ensure that the Web site is using the secure HTTP. You should see the "S" at the end of the HTTP. **Does itsLearning (after you log in) use HTTPS?**

File Transfer Protocol (FTP)

FTP is the network protocol used to transfer data from one computer to another through a network, such as the Internet. FTP is the protocol for exchanging and manipulating files over any TCP-based computer network. A FTP client may connect to a FTP server to manipulate files on that server. Since there are many FTP client and server programs available for different operating systems, FTP is a popular choice for exchanging files independent of the operating systems involved. This web page was uploaded to the web server via an FTP client.

Network Protocol

The network protocol defines rules and conventions for communication between network devices. Protocols for computer networking all generally use packet switching techniques to send and receive messages in the form of packets. Network protocols include mechanisms for:

- Devices to identify and make connections with each other
- Formatting rules that specify how data is packaged into messages sent and received
- Message acknowledgement
- Data compression designed for reliable and/or high-performance network communication

Hundreds of different computer network protocols have been developed each designed for specific purposes and environments. The most common protocols are:

- Ethernet
- LocalTalk
- Token Ring
- FDDI

Ethernet

Ethernet is the most widely used network protocol. Uses an access method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) where each computer listens to the cable before sending anything through the network. If the network is clear, the computer will transmit, but if some other node is already transmitting on the cable, the computer will wait and try again when the line is clear. When two computers attempt to transmit at the same time, a collision occurs, and each computer then backs off and waits a random amount of time before attempting to retransmit Delay caused by collisions and retransmitting is very small and does not normally effect the speed of transmission on the network Allows for linear bus, star, or tree topologies and transmission speed of 10 Mbps (Megabytes).

Fast Ethernet allows for an increased speed of transmission, the Fast Ethernet protocol has developed a new standard that supports 100 Mbps. Fast Ethernet requires the use of different, more expensive network devices and cables.

LocalTalk

Local Talk developed by Apple for Macintosh computers. Method used by LocalTalk is called CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), which is similar to CSMA/CD except that a computer signals its intent to transmit before it actually does so. The Macintosh operating system allows the establishment of a peer-to-peer network without the need for additional software. With the addition of the server version of AppleShare software, a client/server network can be established. Local Talk allows for linear bus, star, or tree topologies and transmission speed is only 230 Kbps (Kilobytes).

Token Ring

Token Ring is a protocol developed by IBM in the mid-1980s. The access method used involves token-passing where computers are connected so that the signal travels around the network from one computer to another in a logical ring. A single electronic token moves around the ring from one computer to the next and if a computer does not have information to transmit, it simply passes the token on to the next workstation. If a computer wishes to transmit and receives an empty token, it attaches data to the token and the token then proceeds around the ring until it comes to the computer for which the data is meant. Taken Ring requires a star-wired ring and transmission speeds are 4 Mbps or 16 Mbps.

Fiber Distributed Data Interface (FDDI)

FDDI is used primarily to interconnect two or more local area networks, often over large distances and access method used by FDDI involves token-passing. Transmission normally occurs on one of the rings; however, if a break occurs, the system keeps information moving by automatically using portions of the second ring to create a new complete ring. FDDI requires a dual ring topology and has transmission speed of 100 Mbps.

Network Security

When personal computer users want to encrypt e-mail or other documents, they turn to public key encryption software called PGP (Pretty Good Privacy) software. Encryption transforms a message so that its contents are hidden from unauthorized readers. Plaintext has not yet been encrypted. An encrypted message is referred to as ciphertext. Encryption methods can be broken by the use of expensive, specialized, code-breaking computers. Public key encryption (PKE) eliminates key-distribution problem, by using one key to encrypt a message and another key to decrypt the message.

Public Key Cryptography: RSA Encryption Algorithm

Wi-Fi Security

Wireless networks are much more susceptible to unauthorized access and use than wired networks. LAN jacking, or war driving, is the practice of intercepting wireless signals by cruising through an area. Our Wi-Fi enabled devices will scan for a network signal. If a Wi-Fi signal is not password protected, then anyone and everyone can use that Wi-Fi connection. Most of us have probably been guilty of lanjacking. If we are away from our own Wi-Fi connection and wish to establish an Internet connection for whatever reason, we will use an unsecured Wi-Fi signal. We sure to protect your own Wi-Fi signal, whether your home connection or your mobile hotspot on a data enabled device, with a strong password. A strong password uses a combination of letters, numbers and symbols and is not easily identifiable. For example, my mom's maiden name is not a good password for me to use. It is easy to figure out especially with most people including that information on their Facebook profiles.

An offshoot of war driving is a gambit called war chalking. Chalkers make chalk marks on outdoor surfaces to indicate wireless networks. They use symbols to indicate passwords for WEPs (Wired Equivalent Privacy). Wireless encryption scrambles data transmitted between wireless devices and then unscrambles the data only on devices that have a valid encryption key. Encryption is activated by using a wireless network key.

Assignment: Cipher Text Assignment and Discussion Board

Directions: Download the Cipher Table from itsLearning. Write a message of at least 25 words. Use the cipher table to encrypt the message and then upload it to the assignment and post to the Cipher Text Discussion Board (only post the encrypted

message. Use your cipher table to then decrypt another classmate's message. Post the plain text of their message as a reply.

Jrrg oxfn dqg ixq!

Review

Resources

If you are having problems viewing this page, opening videos, or accessing the URLs, the direct links are posted below. All assignments are submitted in itsLearning. If you have having problems, contact Mrs. Rush through the itsLearning email client.

WGBH Computer Networks:
http://www.pbslearningmedia.org/asset/ate10_int_networks/

Computer History Museum: http://www.computerhistory.org/timeline/?category=net

LANs vs. WANs presentation: http://www.mrsrush.net/idt/networks/lan-wan.pdf

Warriors on the Net video: http://www.youtube.com/watch?v=n7mtJ3ZV6xM

Public Key Encryption video: http://www.youtube.com/watch?v=wXB-V_Keiu8

Review: https://www.examtime.com/en-US/p/995352

Transcript: http://mrsrush.net/networks/index.pdf

Credits

WiFi icon: http://dryicons.com

Lock icon: http://dryicons.com

Transcript of this lesson