NAME: OKUNUGA AMINAT MAKANJUOLA

MATRIC NO: 20141628

DEPARTMENT: COMPUTER SCIENCE

COURSE TITLE: DATA COMMUNICATIONS AND NETWORK

QUESTIONS:

1. Juxtapose star and bus topology.
2. List and explain five (5) application areas of a network.
3. Discuss comprehensively network protocols (with appropriate references and citations).

QUESTION 1

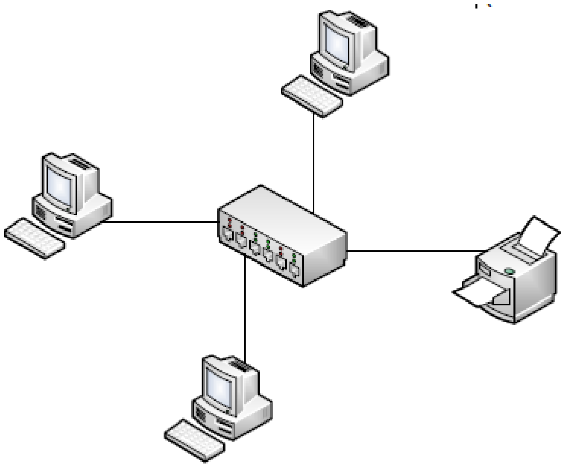
STAR AND BUS TOPOLOGY

Star Topology

In a star topology, all workstations and peripherals are connected to a central connection point. In the star topology, computers are connected by cable segments to centralized component, called a hub or switch.

Signals are transmitted from the sending computer through the hub or switch to all computers on the network. This topology originated in the early days of computing with computers connected to a centralized mainframe computer. It is now a common topology in microcomputer networking. Each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device

Structure of a star topology



The star network offers centralized resources and management. However, because each computer is connected to a central point, this topology requires a great deal of cable in a large network installation. Also, if the central point fails, the entire network goes down.

Advantages of Star Topology

- As compared to Bus topology it gives far much better performance, signals do not necessarily get transmitted to all the workstations. A sent signal reaches the intended destination after passing through no more than 3-4 devices and 2-3 links. Performance of the network is dependent on the capacity of central hub.
- Easy to connect new nodes or devices. In star topology new nodes can be added easily without affecting rest of the network. Similarly, components can also be removed easily.
- Centralized management. It helps in monitoring the network.
- Failure of one node or link does not affect the rest of network. At the same time, it is easy to detect the failure and troubleshoot it.

Disadvantages of Star Topology

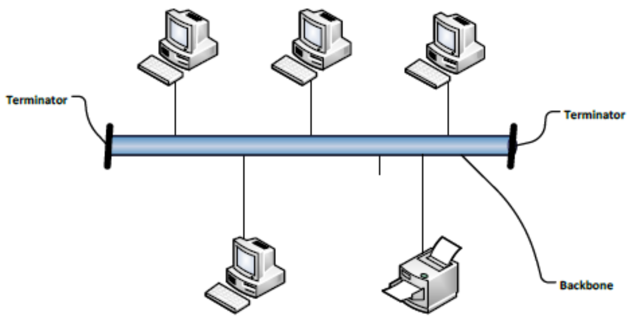
- Too much dependency on central device has its own drawbacks. If it fails whole network goes down.
- The use of hub, a router or a switch as central device increases the overall cost of the network.
- Performance and as well number of nodes which can be added in such topology is depended on capacity of central device.
- The central connection point is not necessarily a server-more typically it is a hub
- Any link can fail without affecting the rest of the network
- It requires a lot of cable to link all devices
- Wireless removes the cable problem
- Device with a failed link would be cut off from the network and unable to receive data

WHILE

Bus topology

The Bus topology consists of a single cable that runs to every work-station. See figure 10. The bus topology is also known as linear bus. In other words, all the nodes (computers and servers) are connected to the single cable (called bus), by the help of interface connectors. This central cable is the back bone of the network and every workstation communicates with the other device through this bus.

Structure of a bus topology



Computers on a bus topology network communicate by addressing data to a particular computer and putting that data on the cable in the form of electronic signals. To understand how computers communicate on a bus you need to be familiar with three concepts:

- **Sending the signal**: Network data in the form of electronic signals is sent to all of the computers on the network; however, the information is accepted only by the computer whose address matches the address encoded in the original signal. Only one computer at a time can send messages.

Because only one computer at a time can send data on a bus network, network performance is affected by the number of computers attached to the bus. The more computers on a bus, the more computers there will be waiting to put data on the bus, and the slower the network.

There is no standard measure for the impact of numbers of computers on any given network. The amount the network slows down is not solely related to the number of computers on the network. It depends on numerous factors including:

Hardware capacities of computers on the network

- Number of times computers on the network transmit data
- Type of applications being run on the network
- Types of cable used on the network
- Distance between computers on the network

The bus is a passive topology. Computers on a bus only listen for data being sent on the network. They are not responsible for moving data from one computer to the next. If one computer fails, it does not affect the rest of the network. In active topology computers regenerate signals and move data along the network.

- **Signal Bounce**: Because the data, or electronic signal, is sent to the entire network, it will travel from one end of the cable to the other. If the signal were allowed to continue uninterrupted, it would keep bouncing back and forth along the cable and prevent other computers from sending signals. Therefore, the signal must be stopped.

- The Terminator: To stop the signal from bouncing, a component called a terminator is placed at each end of the cable to absorb free signals. Absorbing the signal clears the cable so that other computers can send data. Every cable end on the network must be plugged into something. For example, a cable end could be plugged into a computer or a connector to extend the cable length. Any open cable ends-ends not plugged into something – must be terminated to prevent signal bounce.

In bus topology nodes are connected to the bus cable by drop lines and taps. See figure 11. A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason, there is a limit on the number of taps a bus can support and on the distance between those taps.

Advantages of Bus Topology

- Uses a common backbone to connect all network devices
- Backbone functions as a shared communication link which carries network data
- Backbone stops at each end of the network with a special device called a terminator
- Work best with a limited number of devices
- Too many computers are likely to perform poorly
- If backbone cables fail, entire network is unusable
- It is easy to set-up and extend bus network.
- Cable length required for this topology is the least compared to other networks.
- Bus topology very cheap.
- Linear Bus network is mostly used in small networks.

Disadvantages of Bus Topology

- There is a limit on central cable length and number of nodes that can be connected.
- Dependency on central cable in this topology has its disadvantages. If the main cable (i.e. bus) encounters some problem, whole network breaks down.
- Proper termination is required to dump signals. Use of terminators is must.
- It is difficult to detect and troubleshoot fault at individual station.
- Maintenance costs can get higher with time.
- Efficiency of Bus network reduces, as the number of devices connected to it increases.
- It is not suitable for networks with heavy traffic.
- Security is very low because all the computers receive the sent signal from the source.

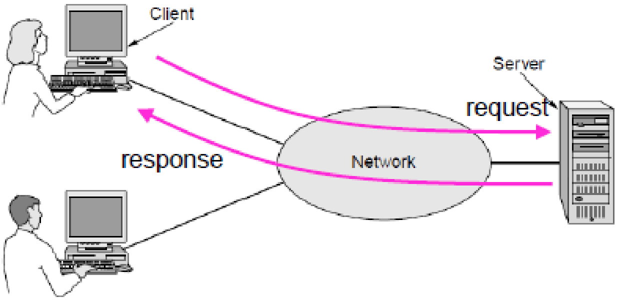
Question 2

Application areas of a network

- Business application
- Mobile application

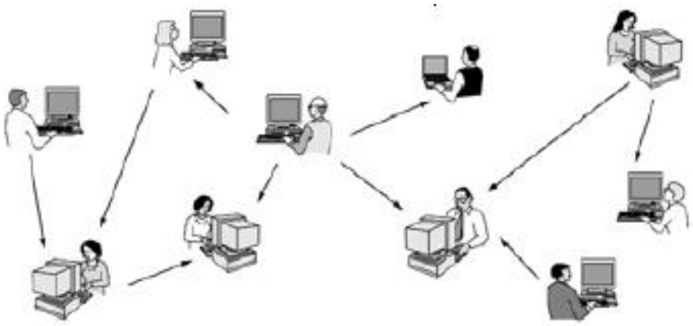
- Home application

Business application: companies use networks and computers for resource sharing with the client-server model. They also use network in communication e.g email, VoIP, and e-commerce.



Mobile applications: Tablets, laptops, and smart phones are popular devices; WiFi hotspots and 3G cellular provide wireless connectivity. Mobile users communicate, e.g., voice and texts, consume content, e.g., video and Web, and use sensors, e.g., GPS.

Home applications: homes contain many networked devices, e.g., computers, TVs, connected to the Internet by cable, DSL, wireless, etc. Home users communicate, e.g., social networks, consume content, e.g., video, and transact, e.g., auctions. Some application uses the peer-to-peer model in which there are no fixed clients and servers:



<u>Question 3</u>

<u>Network Protocols</u>

A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. It defines what is communicated, how it is communicated, and when it is communicated. Without a protocol, two devices may be connected but not communicating, just as a person speaking Igbo cannot be understood by a person who speaks only Yoruba. A communication protocol is a description of the rules that communication devices must follow to communicate with each other. A Protocol is one of the components of a data communications system. Without protocol communication cannot occur. The sending device cannot just send the data and expect the receiving device to receive and further interpret it correctly.

Elements of a Protocol

There are three key elements of a protocol:

a. Syntax is the structure or format of the data. It is the arrangement of data in a particular order. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.

b. Semantics gives the meaning of each section of bits and indicates the interpretation of each section. It also tells what action/decision is to be taken based on the interpretation. For example, does an address identify the route to be taken or the final destination of the message?

c. Timing tells the sender about the readiness of the receiver to receive the data. It tells the sender at what rate the data should be sent to the receiver to avoid overwhelming the receiver. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

Transmission Control Protocol (TCP)

TCP/IP is the basic communication protocol for two or more computers or electronic devices (e.g mobile phone) to communicate with one another on a network setup. TCP/IP stands for Transmission Control Protocol/Internet Protocol. TCP/IP defines how electronic devices (like computers) should be connected to the Internet, and how data should be transmitted between them. TCP/IP is the major protocol in communication network that communication can do without. Inside the TCP/IP standard there are several protocols for handling data communication these are: TCP (Transmission Control Protocol) communication between applications; UDP (User Datagram Protocol) simple communication between applications; IP (Internet Protocol) communication between computers; ICMP (Internet Control Message Protocol) for errors and statistics; DHCP (Dynamic Host Configuration Protocol) for dynamic addressing; and TCP Uses a Fixed Connection.

Transmission Control Protocol: Transmission Control Protocol takes care of the communication between your application software (i.e. your browser) and your network software. TCP is responsible for breaking data down into IP packets before they are sent, and for assembling the packets when they arrive. TCP is for communication between applications. If one application wants to communicate with another via TCP, it sends a communication request. This request must be sent to an exact address. After a "handshake" between the two applications, TCP will set up a "full-duplex" communication between the two applications. The "full-duplex" communication will occupy the communication line between the two computers until it is closed by one of the two applications.

Internet Protocol: Internet Protocol is Connection-Less i.e, it does not occupy the communication line between two computers. The Network Layer protocol for TCP/IP is the Internet Protocol (IP). It uses IP addresses and the subnet mask to determine whether the datagram is on the local or a remote network. If it is on the remote network, the datagram is forwarded to the default gateway which is a router that links to another network. IP keeps track of the number of transverses through each router that the datagram goes through to reach its destination. Each transvers is called a hop. If the hop count exceeds 255 hops, the datagram is removed and the destination considered unreachable. IP reduces the need for network lines. Each line can be used for communication between many different computers at the same time. With IP, messages (or other data) are broken up into small independent "packets" and sent between computers via the Internet. IP is responsible for "routing" each packet to the correct destination.

Special Purpose Protocol

The special purpose protocols are the set of protocols design to perform a single task on communication network system. Some of these protocols and their function are listed below:

i. HTTP - Hyper Text Transfer Protocol: HTTP takes care of the communication between a web server and a web browser. HTTP is used for sending requests from a web client (a browser) to a web server, returning web content (web pages) from the server back to the client.

ii. HTTPS - Secure HTTP: HTTPS takes care of secure communication between a web server and a web browser. HTTPS typically handles credit card transactions and other sensitive data.

iii. SSL - Secure Sockets Layer: The SSL protocol is used for encryption of data for secure data transmission.

iv. MIME - Multi-purpose Internet Mail Extensions: The MIME protocol lets SMTP transmit multimedia files including voice, audio, and binary data across TCP/IP networks.

v. IMAP - Internet Message Access Protocol: IMAP is used for storing and retrieving e-mails.

vi. FTP - File Transfer Protocol: FTP takes care of transmission of files between computers.

vii. NTP - Network Time Protocol: NTP is used to synchronize the time (the clock) between computers.

viii. DHCP - Dynamic Host Configuration Protocol: DHCP is used for allocation of dynamic IP addresses to computers in a network.

ix. SNMP - Simple Network Management Protocol: SNMP is used for administration of computer networks.

x. LDAP - Lightweight Directory Access Protocol: LDAP is used for collecting information about users and e-mail addresses from the internet.

xi. ICMP - Internet Control Message Protocol: ICMP takes care of error-handling in the network.

xii. ARP - Address Resolution Protocol: ARP is used by IP to find the hardware address of a computer network card based on the IP address.

xiii. RARP - Reverse Address Resolution Protocol: RARP is used by IP to find the IP address based on the hardware address of a computer network card.

References

Alberto Leon-Garcial and Indra Widjaja. Communication Networks, Fundmental Concepts and Key Architecture. Second Edition, McGraw-Hill Publishing Company, New dehlhi 2004

Bertsekas, D. and R. Gallager, Data Networks, Prentice-Hall, Englewood Cliffs, 1992

Clack, M. P., Network and Telecommunication: Design and Operation, John Willey and Sons, New York, 1997.

Jain, B. N. and A.K. Agrawala. Open System Interconnection: Its architecture and Protocol. McGraw-Hill. New York 1993

William Buchanan, Distributed Systems and Networks, McGraw-Hill Publishing Company, 2000.

Yekini and Lawal 2010, Introduction to ICT and data Processing, Hasfem Publication Nigeria.
Yekini et al, 2007. Fundamental of Computing, Hasfem Publication Nigeria.

Bello, O and Adebari, F. A. (2012) “Data communication and Networking”, Tony Terry Prints, Lagos, Nigeria.