NATIONAL OPEN UNIVERSITY OF NIGERIA

SCHOOL OF SCIENCE & TECHNOLOGY

CIT 622 – COMPUTER NETWORKS (Marking Scheme)

1a. What is a network operating system?

A network operating system (NOS) is a computer operating system that is designed primarily to support workstation, personal computer, and, in some instances, older terminal that are connected on a local area network (LAN).
5 marks

b. What does a network operating system provide?

A network operating system provides printer sharing, common file system and database sharing, application sharing, and the ability to manage a network name directory, security, and other housekeeping aspects of a network. 5 marks

c. Explain the Peer-to-Peer and Client/Server network operating systems

Peer-to-Peer

Peer-to-peer network operating systems allow users to share resources and files located on their computers and to access shared resources found on other computers. However, they do not have a file server or a centralized management source. In a peer-to-peer network, all computers are considered equal; they all have the same abilities to use the resources available on the network. Peer-to-peer networks are designed primarily for small to medium local area networks.

Client/Server

Client/server network operating systems allow the network to centralize functions and applications in one or more dedicated file servers. The file servers become the heart of the system, providing access to resources and providing security. Individual workstations (clients) have access to the resources available on the file servers. The network operating system provides the mechanism to integrate all the components of the network and allow multiple users to simultaneously share the same resources irrespective of physical location. 10 marks

2a. Define Protocol.

b.. Explain the key elements of a protocol.

c. Briefly discuss Carrier Sense on Multi-Access Networks (CSMA) and Carrier Sense Multiple Access with Collision Detect (CSMA/CD)..

A protocol is a set of rules that governs the communications between computers on a network 4 marks

The key elements of a protocol are syntax, semantics, and timing.

Syntax

Syntax refers to the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the first eight bits of data to be the address of the sender, the second eight bits to be the address of the receiver, and the rest of the stream to be the message itself.

Semantics

Semantics refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation. For example, does an address identify the route to be taken or the final destination of the message?

Timing

Timing refers to two characteristics: when data should be sent and how fast they can be sent. 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 data will be largely lost. 6 marks
.

Carrier Sense on Multi-Access Networks (CSMA)

The most interesting aspect of Ethernet is the mechanism used to coordinate transmission. An Ethernet network does not have a centralized controller that tells each computer how to take turns using the shared cable. Instead, all computers attached to an Ethernet participate in a distributed coordination scheme called Carrier Sense Multiple Access (CSMA). The scheme uses electrical activity on the cable to determine status. When no computer is sending a frame, the ether does not contain electrical signals. During frame transmission, however, a sender transmits electrical signals used to encode bits. Although the signals differ slightly from the carrier waves, they are informally called a carrier. Thus, to determine whether the cable is currently being used, a computer can check for a carrier. If no carrier is present, the computer can transmit a frame. If a carrier is present, the computer must wait for the sender to finish before proceeding. Technically, checking for a carrier wave is called carrier sense, and the idea of using the presence of a signal to determine when to transmit is called Carrier Sense Multiple Access (CSMA).

Carrier Sense Multiple Access with Collision Detect (CSMA/CD)

Because CSMA allows each computer to determine whether a shared cable is already in use by another computer, it prevents a computer from interrupting an ongoing transmission. However, CSMA cannot prevent all possible conflicts. To understand why, imagine what happens if two computers at opposite ends of an idle cable both have a frame ready to send at the same time. When they check for a carrier, both stations find the cable idle, and both start to send frames simultaneously. The signals travel at approximately 70% of the speed of light, and when the signals transmitted by two computers reach the same point on the cable, they interfere with each other.

The interference between two signals is called a collision. Although a collision does not harm the hardware, it produces a garbled transmission that prevents either of the two frames from being received correctly. To ensure that no other computer transmits simultaneously, the Ethernet standard requires a sending station to monitor signals on the cable. If the signal on the cable differs from the signal that the station is sending, it means that a collision has occurred. Whenever a collision is detected, a sending station immediately stops transmitting. Technically, monitoring a cable during transmission is known as Collision Detect {CD), and the Ethernet mechanism is known as Carrier Sense Multiple Access with Collision Detect (CSMA/CD).

CSMA/CD does more than merely detect collisions - it also recovers from them. After a collision occurs, a computer must wait for the cable to become idle again before transmitting a frame. However, if the computers begin to transmit as soon as the ether becomes idle another collision will occur. To avoid multiple collisions, Ethernet requires each computer to delay after a collision before attempting to retransmit. The standard specifies a maximum delay, d, and forces each computer to choose a random delay less than d. In most cases, when a computer chooses a delay at random, it will select a value that differs from any of the values chosen by the other computers – the computer that chooses the smallest delay will proceed to send a frame and the network will return to normal operation.

If two or more computers happen to choose nearly the same amount of delay after a collision, they will both begin to transmit at nearly the same time, producing a second collision. To avoid a sequence of collisions, Ethernet requires each computer to double the range from which a delay is chosen after each collision. Thus, a computer chooses a random delay from 0 to d after one collision, a random delay between 0 and 2d after a second collision, between 0 and 4d after a third, and soon after a few collisions, the range from which a random value is chosen becomes large, and the probability is high that some computer will choose a short delay and transmit without a collision.

Technically, doubling the range of the random delay after each collision is known as binary exponential back off. In essence, exponential back off means that an Ethernet can recover quickly after a collision because each computer agrees to wait longer times between attempts when the cable becomes busy. In the unlikely event that two or more computers choose delays that are approximately equal, exponential back off guarantees that contention for the cable will be reduced after a few collisions.

Computers attached to an Ethernet use CSMA/CD in which a computer waits for the ether lo be idle before transmitting a frame. If two computers transmit simultaneously, a collision occurs: the computers use exponential back off to choose which computer will proceed. Each computer' delays a random time before trying to transmit again, and then doubles the delay for each successive collision. 10 marks

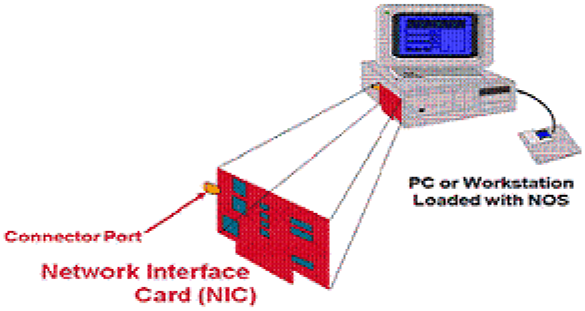
3. Discuss the four components of LAN

COMPONENTS OF LAN

- Network operating system (NOS)

In order for computers to be able to communicate with each other, they must first have the networking software that tells them how to do so. Without the software, the system will function simply as a “standalone,” unable to utilize any of the resources on the network. Network operating software may by installed by the factory, eliminating the need for you to purchase it, (for example AppleTalk), or you may install it yourself.

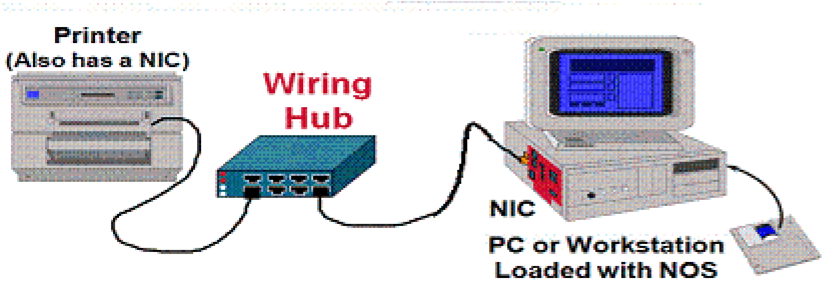
- Network interface card (NIC)



Network interface card

In addition to network operating software, each network device must also have a network interface card. These cards today are also referred to as adapters, as in “Ethernet adapter card” or “Token Ring adapter card.” The NIC card amplifies electronic signals which are generally very weak within the computer system itself. The NIC is also responsible for packaging data for transmission, and for controlling access to the network cable. When the data is packaged properly, and the timing is right, the NIC will push the data stream onto the cable. The NIC also provides the physical connection between the computer and the transmission cable (also called “media”). This connection is made through the connector port. Examples of transmission media are Ethernet, Token Ring, and FDDI.

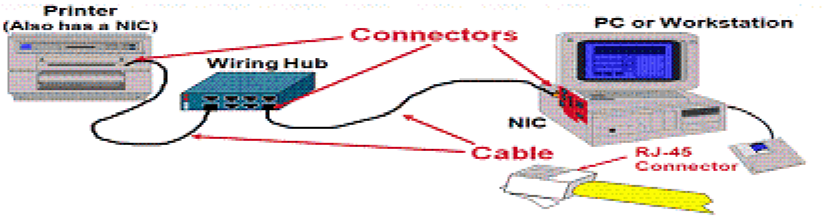
Wiring Hub



Wiring Hub

In order to have a network, you must have at least two devices that communicate with each other. In this simple model, it is a computer and a printer. The printer also has an NIC installed (for example, an HP Jet Direct card), which in turn is plugged into a wiring hub. The computer system is also plugged into the hub, which facilitates communication between the two devices. Additional components (such as a server, a few more PCs, and a scanner) may be connected to the hub. With this connection, all network components would have access to all other network components. The benefit of building this network is that by sharing resources a company can afford higher quality components. For example, instead of providing an inkjet printer for every PC, a company may purchase a laser printer (which is faster, higher capacity, and higher quality than the inkjet) to attach to a network. Then, all computers on that network have access to the higher quality printer.

- Cables or Transmission Media



Cable or Transmission Media

The wires connecting the various devices together are referred to as cables.

- Cable prices range from inexpensive to very costly and can comprise of a significant

  cost of the network itself.

- Cables are one example of transmission media. Media are various physical environments through which transmission signals pass. Common network media include twisted-pair, coaxial cable, fiber-optic cable, and the atmosphere (through

5 marks each

4a. Explain IP addressing

An IP address is a numeric identifier assigned to each machine on an IP network. It designates the specific location of a device on the network. An IP address is a software address, not a hardware address- the latter is hard-coded on a Network Interface Card (NIC) and used for finding hosts on a local network. IP addressing was designed to allow a host on one network to communicate with a host on a different network, regardless of the type of LANs the hosts are participating in. 8 marks

b. List the two IP addressing schemes

There are two IP addressing schemes:

1. Hierarchical IP addressing
2. Private IP Addressing

6 marks

c. What is addressing designed to achieve?

Addressing was designed to allow a host on one network to communicate with a host on a different network, regardless of the type of LANs the hosts are participating in. 6 mks

5. Outline eight of the key issues to be trashed out carefully before setting up computer network

KEY ISSUES TO COMPUTER NETWORK

The following are the major key issues to be trashed out very carefully before we go for a computer network:

1. *Nature of Nodes* -Whether participating nodes are homogeneous or heterogeneous in nature?
2. *Topology* - Which of the computer topology has to be followed? Computer topology accounts for the physical arrangement of participating computers in the network.
3. *Interconnection Type* - Whether interconnection type is point-to-point, multi-point, or broadcast type.
4. *Reliability* - How reliable our network is? Reliability aspect includes error rate, redundancy and recovery procedures.
5. *Channel Capacity Allocation* - Whether allocation of channel capacity is time-division or frequency division?
6. *Routing Techniques* - Whether message between nodes are to be routed through: Deterministic, Stochastic, and Distributed routing techniques?
7. *Models* - Which of the models i.e. analytical models, queuing models, simulation models, measurement and validation models are applicable?
8. *Channel Capacity* - What are the channel capacities of the communication lines connecting nodes?
9. *Access* - Whether computer access in the network is direct-access or through a sub-network?
10. *Protocols* - What levels, standards and formats are to be followed while establishing communication between participating nodes?
11. *Performance* - How is higher performance of computer network achieved? Response time, time to connect, resource utilization, etc. contribute towards performance of computer network.
12. *Control* - Whether centralized control, distributed control or hierarchical control of participating nodes of computer network is suitable?

20 marks

6a. Explain network topology concept

The term topology refers to the way a network is laid out, either physically or logically. The physical topology of a network refers to the configuration of cables, computers, and other peripherals while the logical topology is the method used to pass information between workstations. Two or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to each other.

5 marks

b. List five basic topologies

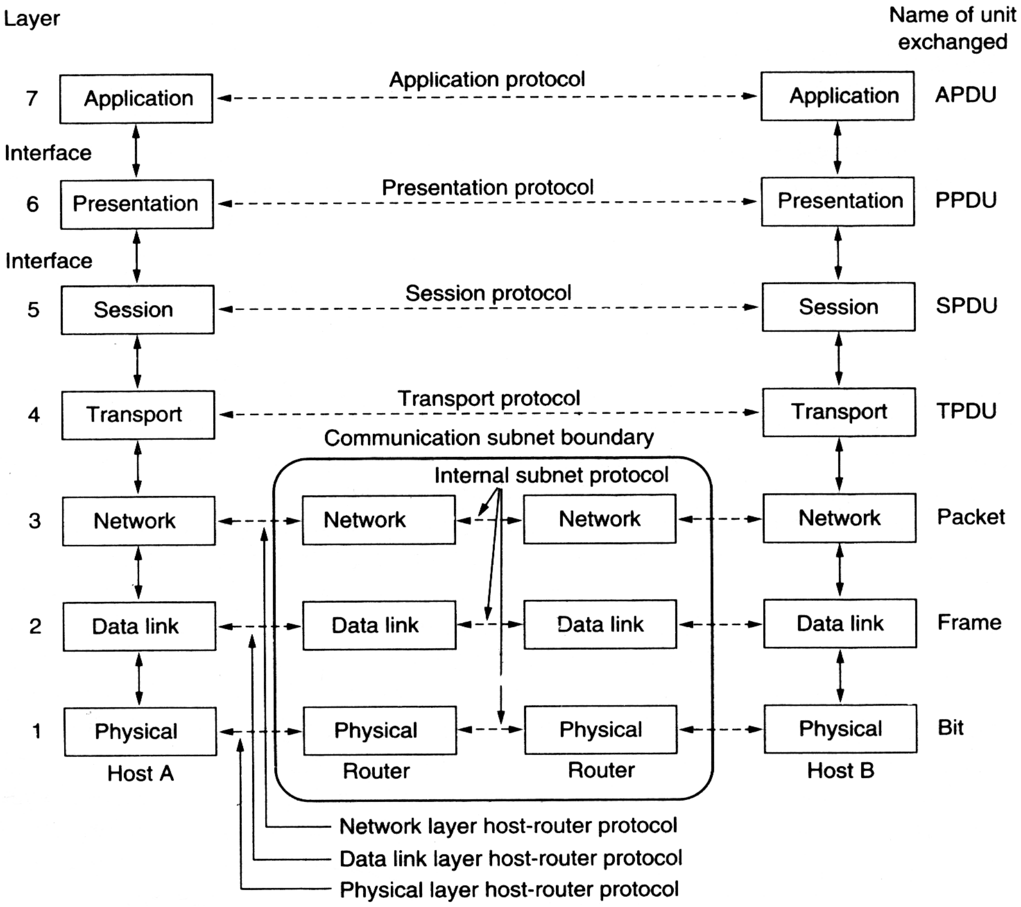
The five basic topologies possible are: mesh, star, tree, bus, and ring. 5 marks

c. What is the key disadvantage of a physically direct-wired LAN? Explain how a star-wired LAN can be used to correct the problem.

Fault detection and isolation are very difficult in a large (large span and large number of stations) direct-wired LAN. To find and isolate a fault one must literally "walk the wire". 5 marks

In a star wired LAN faults can be detected and isolated in a central location – the wiring closet. To detect and isolate a fault in a wiring closet, individual lobes of the LAN can be unplugged until the LAN returns to operation. This can be automated. 5 marks

7a. Sketch the OSI model and describe the function of the layers with one sentence for each layer.



The OSI Reference Model 7 marks

OSI layers: Applications, Presentation, Session, Transport, Network, Data Link, and Physical (top to bottom).

Application – provides access to user applications

Presentation – provides data independence

Session – manages end-to-end connections

Transport – provides reliable end-to-end data transport

Network – maintains point-to-point connections

Data Link – provide reliable point-to-point data transport

Physical – transmission of bit stream 7 marks

b. Briefly describe the characteristics of the OSI 7 layer model

CHARACTERISTICS OF THE OSI 7 LAYERS MODEL

Layers 7 to 4 - deal with end to end communications between data source and destinations.

Layers 3 to 1 - deal with communications between network devices.

On the other hand, the seven layers of the OSI model can be divided into two groups: upper layers (layers 7, 6 & 5) and lower layers (layers 4, 3, 2, 1). The upper layers of the OSI model deal with application issues and generally are implemented only in software. The highest layer, the application layer, is closest to the end user. The lower layers of the OSI model handle data transport issues. The physical layer and the data link layer are implemented in hardware and software. The lowest layer, the physical layer, is closest to the physical network medium (the wires, for example) and is responsible for placing data on the medium. 6 marks