(Please write your Roll No. immediately) ROLL NO. ----------

END TERM EXAMINATION (MODELQUESTION PAPER WITH ANSWERS)

SIXTH SEMESTER [B.TECH] MAY-JUNE 2014

Paper Code: ETCS306/ETIT306 ***Subject: Computer Networks***

Time: 3 Hours ***Maximum Marks: 75***

Note: Q. no.1 is compulsory. Attempt one question from each unit.

Q1. (a) What is the difference between baseband and broadband? (2.5*10)
(b)What is the difference between TCP and UDP?
(c)Compare UTP and STP cable.
(d)Why OSI model called "Open System Interconnection"?
(e)What is the purpose of Bit Stuffing?
(f)Define the term Connection-oriented communication and Connection –less communication.
(g)Define protocols and what are key elements of protocol?
(h) Explain the concept of layered task of networking.
(i) What is MAC address?
(j) What is difference between physical and logical topology?

UNIT-I

Q2. (a) What are the different types of transmission impairments? (4.5)
(b) Define Masking. What is the difference between boundary level masking and non-boundary level masking? (3)
(c) Distinguish between adaptive and non adaptive routing algorithms. (5)

Q3. (a) what is an IP address? Discuss the class field in IP address. (4.5)
(b)What is the difference between service point address, logical address and physical address?(3)
(c) What is difference between Distance Vector Routing Protocols and Link State Routing Protocols. (5)

UNIT-II

Q4. (a)Explain leaky bucket algorithm and how traffic congestion can be reduced. (5)
(b) Explain broadcast network, point to point network and Multipoint networks. (5)
(c) Differentiate between amplifier and repeater. (2.5)

Q5. (a) Explain pure aloha and slotted aloha. (4.5)
(b) Define ATM. What are advantages of ATM Network? (4)
(c) What is ISDN? Explain types of services provided by ISDN. (4)

UNIT-III

Q6. (a) A company is granted a site address 201.70.64.0. The company needs six subnets. Design the subnets. (6.5)

(b) Explain Sliding Window Protocol in details. (6)

Q7. (a) Explain IEEE 802.3 frame format. (4)

(b) Explain comparison of virtual-circuit and datagram networks. (4)

(c) Compare and contrast FDMA, TDMA and CDMA techniques. 4.5)

UNIT-IV

Q8. (a)Explain different types of computer networks. (6.5)

(b) Explain function of token ring. (6)

Q9. (a)Explain function of token bus. (4)

(b)What is the advantage of token passing protocol over CSMA/CD protocol? (3.5)

(c) What are the drawbacks of token ring topology? (3)

(d)What role the active token monitor performs? (2)

ANSWERS

1(a): In Baseband, data is sent as digital signals through the media as a single channel that uses the entire bandwidth of the media. Baseband communication is bi-directional, which means that the same channel can be used to send and receive signals. In Baseband, frequency-division multiplexing is not possible.

Broadband sends information in the form of an analog signal. Each transmission is assigned to a portion of the bandwidth; hence multiple transmissions are possible at the same time. Broadband communication is unidirectional, so in order to send and receive, two pathways are needed. This can be accomplished either by assigning a frequency for sending and assigning a frequency for receiving along the same cable or by using two cables, one for sending and one for receiving. In broadband frequency-division multiplexing is possible.

(b) Difference between Transmission Control Protocol (TCP) and User Datagram Protocol (UDP):

Transmission Control Protocol (TCP)

1) Transmission Control Protocol (TCP) is a connection oriented protocol, which means the devices should open a connection before transmitting data and should close the connection gracefully after transmitting the data.
2) Transmission Control Protocol (TCP) assures reliable delivery of data to the destination.
3) Transmission Control Protocol (TCP) protocol provides extensive error checking mechanisms such as flow control and acknowledgment of data.
4) Sequencing of data is a feature of Transmission Control Protocol (TCP).
5) Delivery of data is guaranteed if you are using Transmission Control Protocol (TCP).
6) Transmission Control Protocol (TCP) is comparatively slow because of these extensive error checking mechanisms
7) Multiplexing and Demultiplexing is possible in Transmission Control Protocol (TCP) using TCP port numbers.
8) Retransmission of lost packets is possible in Transmission Control Protocol (TCP).

User Datagram Protocol (UDP)

1) User Datagram Protocol (UDP) is Datagram oriented protocol with no overhead for opening a connection (using three-way handshake), maintaining a connection, and closing (terminating) a connection.
2) User Datagram Protocol (UDP) is efficient for broadcast/multicast type of network transmission.
3) User Datagram Protocol (UDP) has only the basic error checking mechanism using checksums.
4) There is no sequencing of data in User Datagram Protocol (UDP).

5) The delivery of data cannot be guaranteed in User Datagram Protocol (UDP).
6) User Datagram Protocol (UDP) is faster, simpler and more efficient than TCP. However, User Datagram Protocol (UDP) it is less robust then TCP
7) Multiplexing and Demultiplexing is possible in User Datagram Protocol (UDP) using UDP port numbers.
8) There is no retransmission of lost packets in User Datagram Protocol (UDP).

(c)

- STP cables are shielded while UTP cables are unshielded
- STP cables are more immune to interference and noise than UTP cables
- STP cables are better at maximizing bandwidth compared to UTP cables
- STP cable cost more per meter compared to UTP cables
- STP cables are heavier per meter compared to UTP cables
- UTP cables are more prevalent in *(Small office/home office)* SOHO networks while STP is used in more high-end applications.

(d) OSI stands for open system interconnection model which defines the networking frameworks. It is called open system because it was intended to be used by all vendors. The OSI standard was meant to improve networking.

(e) Bit stuffing is used to distinguish beginning and ending flags from information.

(f) Connection-oriented communication includes the steps of setting up a call from one computer to another, transmitting/receiving data, and then releasing the call, just like a voice phone call. However, the network connecting the computers is a packet switched network, unlike the phone system's circuit switched network. Connectionless service is typically provided by the TCP.

Connectionless communication is just packet switching where no call establishment and release occur. A message is broken into packets, and each packet is transferred separately. Moreover, the packets can travel different route to the destination since there is no connection. Connectionless service is typically provided by the UDP (User Datagram Protocol).

(g) A protocol can be defined as a set of rules determining the format and transmission of data or a set of rules that governs data communication. A protocol defines what is going to be communicated. The key elements of protocol are syntax, semantics and timing.

(h) The main objective of a computer network is to be able to transfer the data from sender to receiver. This task can be done by breaking it into small sub tasks, each of which is well defined. Each subtask will have its own process or processes to do and will take specific inputs and give

specific outputs to the subtask before or after it. In more technical terms we can call these sub tasks as layers. In general, every task or job can be done by dividing it into sub task or layers.

(i) It is the 48 bit hardware address of LAN card. MAC address is usually stored in ROM on the network adapter card and it is unique.

(j) A physical topology describes how devices are physically cabled together. A logical topology describes how devices communicate across the physical topology.

UNIT-I

2(a): TRANSMISSION IMPAIRMENT

Signals travel through transmission media, which are not perfect. The imperfection causes signal impairment. This means that the signal at the beginning of the medium is not the same as the signal at the end of the medium. What is sent is not what is received. Three causes of impairment are attenuation, distortion, and noise.

Attenuation

Attenuation means a loss of energy. When a signal, simple or composite, travels through a medium, it loses some of its energy in overcoming the resistance of the medium. That is why a wire carrying electric signals gets warm, if not hot, after a while. Some of the electrical energy in the signal is converted to heat. To compensate for this loss, amplifiers are used to amplify the signal.

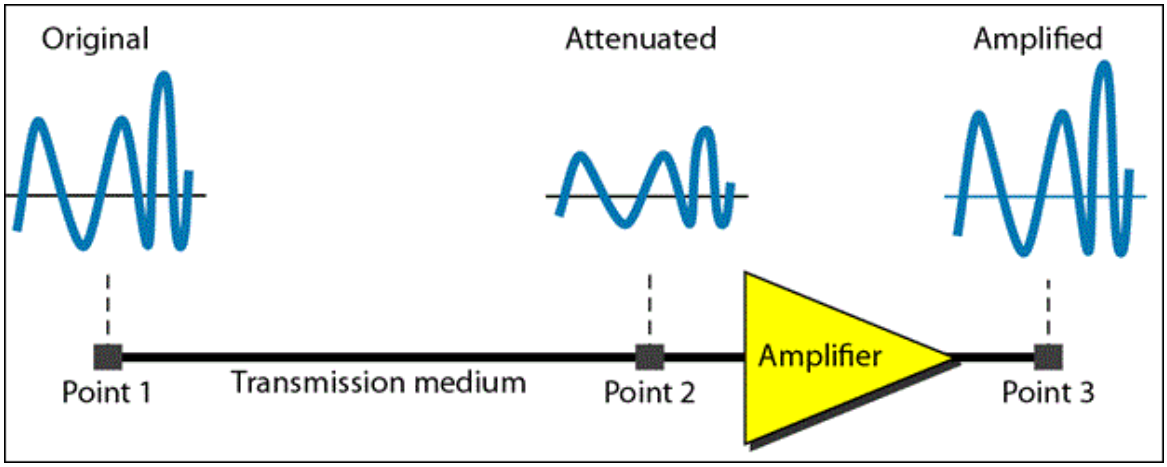


Fig. 2 (a): Attenuation

Distortion

Distortion means that the signal changes its form or shape. Distortion can occur in a composite signal made of different frequencies. Each signal component has its own propagation speed through a medium and, therefore, its own delay in arriving at the final destination. Differences in delay may create a difference in phase if the delay is not exactly the same as the period duration.

In other words, signal components at the receiver have phases different from what they had at the sender. The shape of the composite signal is therefore not the same.

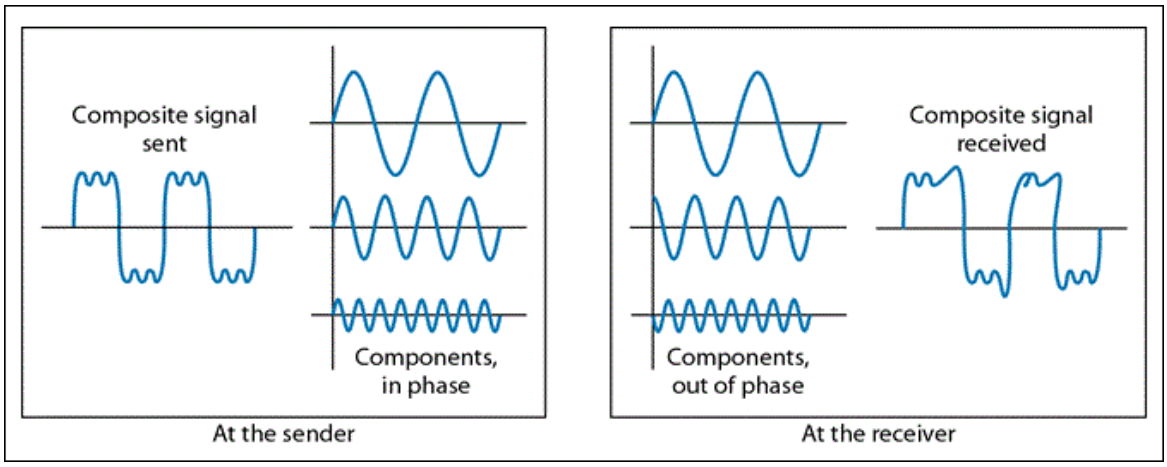


Fig. 2 (b): Distortion

Noise

Noise is another cause of impairment. Several types of noise, such as thermal noise, induced noise, crosstalk, and impulse noise, may corrupt the signal. Thermal noise is the random motion of electrons in a wire which creates an extra signal not originally sent by the transmitter. Induced noise comes from sources such as motors and appliances. These devices act as a sending antenna, and the transmission medium acts as the receiving antenna. Crosstalk is the effect of one wire on the other. One wire acts as a sending antenna and the other as the receiving antenna. Impulse noise is a spike (a signal with high energy in a very short time) that comes from power lines, lightning, and so on.

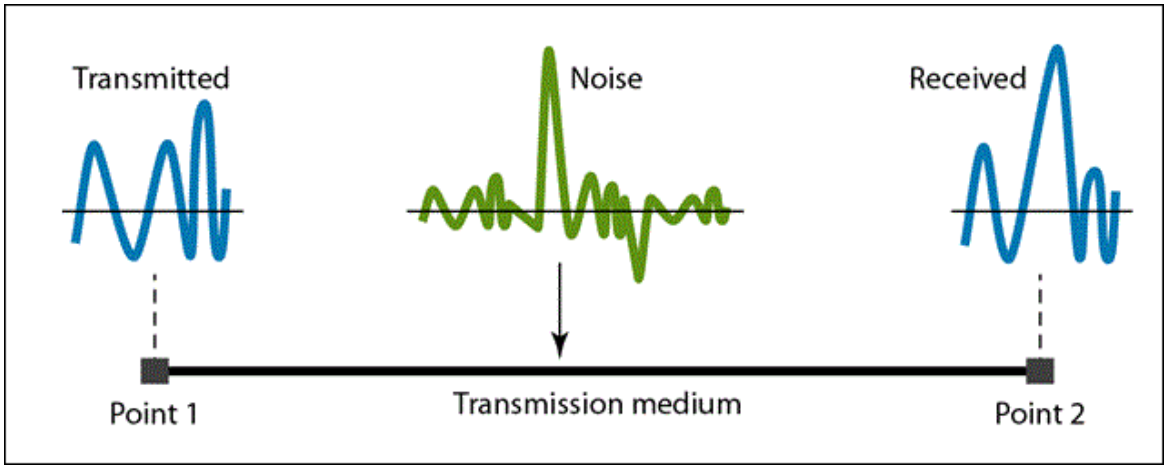


Fig. 2 (b): Noise

(b) Masking is a process that extracts the address of the physical network from an IP address.
Boundary level Masking: If the masking is at the boundary level, the mask numbers are either 255 or 0, finding the sub network address is very easy.

Non Boundary level Masking: If the masking is not at the boundary level, the mask numbers are not just 255 or 0, finding the sub network address involves using the bitwise AND operators.

(c) Non adaptive Routing:
Once a pathway to a destination has been selected the router sends all packets for that destination along that one route. The routing decisions are not based on the condition or topology of the networks.

Adaptive Routing:
Router may select a new route for each packet (even packets belonging to the same transmission) The routing decisions are based on the condition or topology of the networks.

3(a):
An IP address is a 32 - bit address that uniquely and universally define the connection of a host or a router to the Internet. The sender must know the IP address of the destination computer before sending a packet.
If the address is given in binary notation, the first few bits can tell us the class of the address.
Class A - 0
Class B - 10
Class C - 110
Class D - 1110
Class E - 1111

When the address is given in dotted decimal notation, then look at the first byte to determine the class of the address.
Class A - 0 to 127
Class B – 128 to 191
Class C – 192 to 223
Class D – 224 to 239
Class E – 240 to 255

(b)

Service point addressing	**Logical addressing**	**Physical addressing**
The transport layer header includes a type of address called a service point address	If a packet passes the network boundary we need another addressing to differentiate the	If the frames are to be distributed to different systems on the network, the

or port address, which makes a data delivery from a specific process on one computer to a specific process on another computer.	source and destination systems. The network layer adds a header, which indicate the logical address of the sender and receiver.	data link layer adds the header, which defines the source machine's address and the destination machine's address.

(c) Difference between Distance Vector Routing Protocol and Link State Routing Protocol:

Distance Vector Routing

- Entire routing table is sent as an update
- Distance vector protocol send periodic update at every 30 or 90 second
- Update are broadcasted
- Updates are sent to directly connected neighbor only
- Routers don't have end to end visibility of entire network.
- Distance vector routing protocol network may have patch in network carrying wrong information
- It is proned to routing loops
- Routing loop avoidance Mechanism used are as below :

1>Max Hop Count
2> Split horizon
3> Route poisoning
4> Hold down Timer

- Distance vector routing protocol has slow convergence due to periodic update. Eg. **RIP**

Link State Routing

- Updates are incremental & entire routing table is not sent as update
- Updates are triggered not periodic
- Updates are multicasted
- Update are sent to entire network & to just directly connected neighbor
- Updates are carry SPF tree information & SPF cost Calculation information of entire topology
- Routers have visibility of entire network of that area only.
- No routing loops
- Convergence is fast because of triggered updates.
- Eg. : **OSPF**

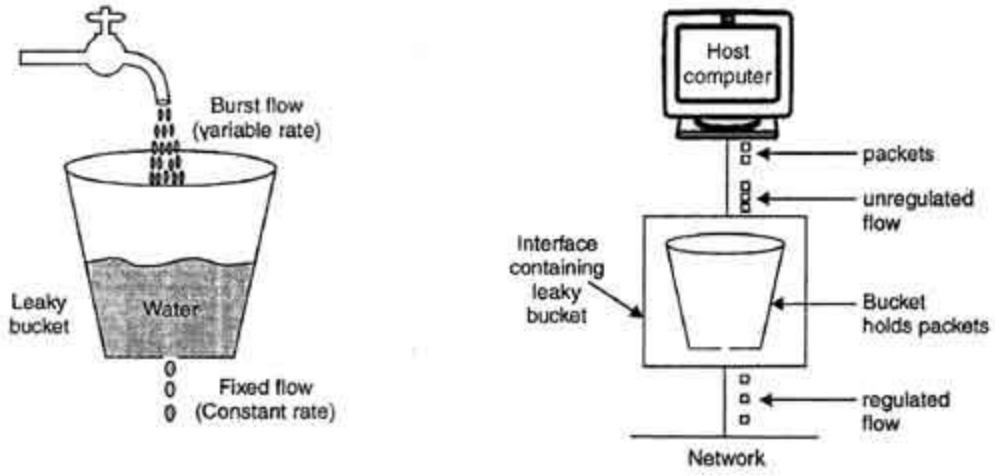
4(a): Leaky Bucket Algorithm

• It is a traffic shaping mechanism that controls the amount and the rate of the traffic sent to the network.

• A leaky bucket algorithm shapes bursty traffic into fixed rate traffic by averaging the data rate.

• Imagine a bucket with a small hole at the bottom.

• The rate at which the water is poured into the bucket is not fixed and can vary but it leaks from the bucket at a constant rate. Thus (as long as water is present in bucket), the rate at which the water leaks does not depend on the rate at which the water is input to the bucket.



(a) A leaky bucket with water (b) A leaky bucket with packets

- Also, when the bucket is full, any additional water that enters into the bucket spills over the sides and is lost.
- The same concept can be applied to packets in the network.

(b) Broadcast Network: A computer network which has a single communication channel. A packet sent by one computer is received by all the others computers on the network. In telecommunication and information theory, broadcasting refers to a method of transferring a message to all recipients simultaneously. Broadcasting can be performed as a high level operation in a program, for example broadcasting Message Passing Interface, or it may be a low level networking operation, for example broadcasting on Ethernet.

Point to Point Network: A simple Point to Point Network is a permanent link between two endpoints. A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible. When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

Multipoint Network: A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link. In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.

(c) A repeater is an electronic device that receives a signal and retransmits it at a higher level or higher power. A repeater does not amplify the signal it regenerates the signal. An amplifier is a device for increasing the power of a signal by increasing the amplitude of electrical signals.

5(a): Pure ALOHA

• In pure ALOHA, the stations transmit frames whenever they have data to send. When two or more stations transmit simultaneously, there is collision and the frames are destroyed.

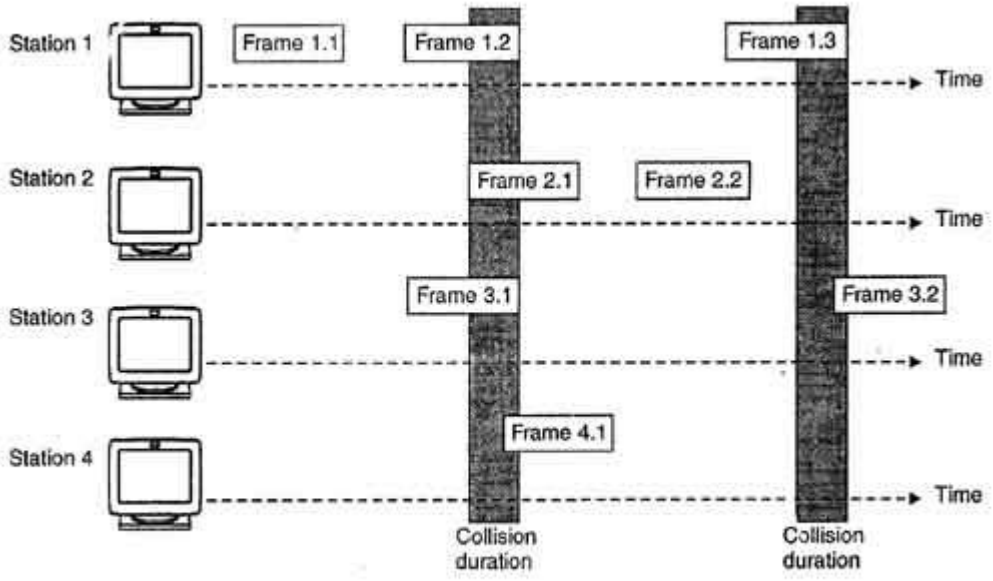
• In pure ALOHA, whenever any station transmits a frame, it expects the acknowledgement from the receiver.

• If acknowledgement is not received within specified time, the station assumes that the frame (or acknowledgement) has been destroyed.

• If the frame is destroyed because of collision the station waits for a random amount of time and sends it again. This waiting time must be random otherwise same frames will collide again and again.

• Therefore pure ALOHA dictates that when time-out period passes, each station must wait for a random amount of time before resending its frame. This randomness will help avoid more collisions.

• Figure shows an example of frame collisions in pure ALOHA.



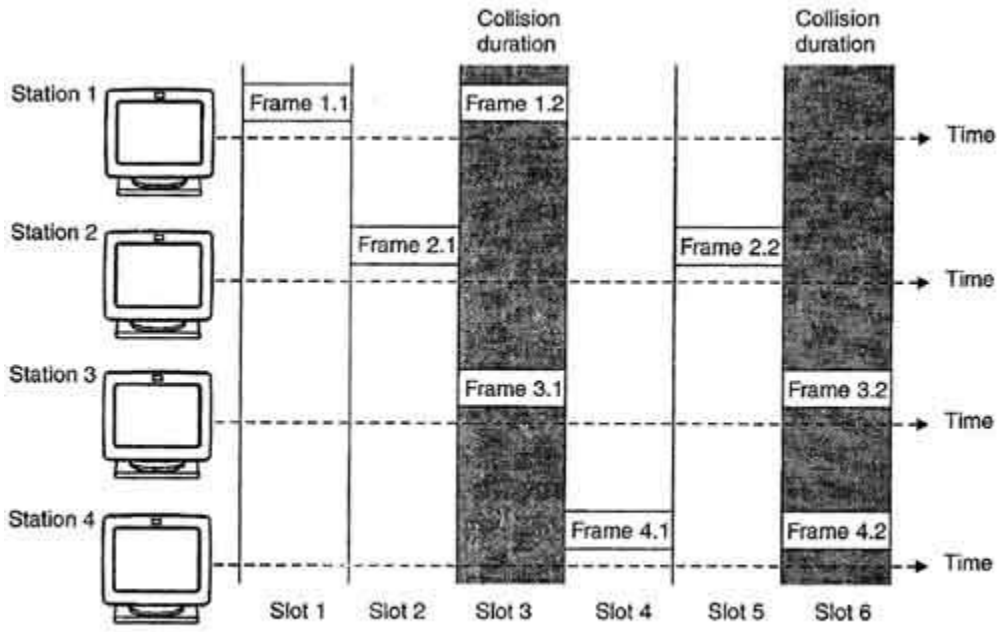
Frames in Pure ALOHA

• In fig there are four stations that contended with one another for access to shared channel. All these stations are transmitting frames. Some of these frames collide because multiple frames are in contention for the shared channel. Only two frames, frame 1.1 and frame 2.2 survive. All other frames are destroyed.

• Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be damaged. If first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted.

Slotted ALOHA

• Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.
• In slotted ALOHA, the time of the shared channel is divided into discrete intervals called slots.
• The stations can send a frame only at the beginning of the slot and only one frame is sent in each slot.



Frames in Slotted ALOHA

• In slotted ALOHA, if any station is not able to place the frame onto the channel at the beginning of the slot *i.e.*it misses the time slot then the station has to wait until the beginning of the next time slot.
• In slotted ALOHA, there is still a possibility of collision if two stations try to send at the beginning of the same time slot as shown in fig.
• Slotted ALOHA still has an edge over pure ALOHA as chances of collision are reduced to one-half.

(b) "Asynchronous Transfer Mode", is a high-speed network technology that supports the transportation of voice, data, and video signals over a single stream. ATM combines both circuit and packet switching methods into one flexible technology that makes for simple network processing functions. That digital data is encoded in the form of small fixed size cells (53-byte

units) instead of the variable sized packets used by Internet Protocol or Ethernet. This ensures that the packets can be sent quickly and easily. ATM is connection oriented, which means that data sent through the ATM network will always follow the same pre-defined path with the data arriving in the order it was sent.

Advantages of ATM Network

The high-level benefits delivered through ATM services deployed on ATM technology using international ATM standards can be summarized as follows:

• Dynamic bandwidth for bursty traffic meeting application needs and delivering high utilization of networking resources; most applications are or can be viewed as inherently bursty, for example voice is bursty, as both parties are neither speaking at once nor all the time; video is bursty, as the amount of motion and required resolution varies over time.

• Smaller header with respect to the data to make the efficient use of bandwidth.

• **Can handle mixed network traffic very efficiently:** Variety of packet sizes makes traffic unpredictable. All network equipments should incorporate elaborate software systems to manage the various sizes of packets. ATM handles these problems efficiently with the fixed size cell.

• **Cell network:** All data is loaded into identical cells that can be transmitted with complete predictability and uniformity.

(C) Integrated Services Digital Network is a set of digital transmission protocols defined by the international standards body for telecommunications, the ITU-T (previously called the CCITT). These protocols are accepted as standards by virtually every telecommunications carrier all over the world. ISDN complements the traditional telephone system so that a single pair of telephone wires is capable of carrying voice and data simultaneously. It is a fully digital network where all devices and applications present themselves in a digital form. The essential difference between ISDN and the conventional telephone system is that it is digital not analogue. Information travels as bits rather than as waves. In addition, it also allows multiple streams of these bits to occupy the same connection, providing the user with greater versatility of services.

ISDN Services: There are two kinds of services provided by ISDN.

Network Services:

• Network Services define how the user and the network interact with each other in order to manage calls.

• The user can use Network Services to request the network to perform functions such as making and clearing calls, transferring calls to another user, and so on.

• This activity is known as signaling.

For example: setting up calls and disconnecting them

Bearer Services:

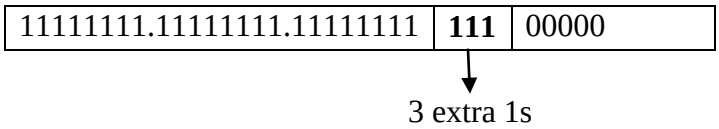
• Bearer services carry the call activity that the user is performing at any given moment.

• This includes voice calls, fax and modem calls, and connections to the Internet.

• Broadly speaking, there are two forms of bearer service.

- Structured Data - the information passing over the bearer service is in a format that is understood by the network. Voice is an example of structured data. Because the network knows that the connection carrying voice, it can convert the data into an analogue signal in the event that the call is connected to an ordinary analogue phone.
- Unstructured Data - the format of the information is not understood by the network, but is understood by the two users at either end of the service.

6(a): This is a class C network. Therefore, the default mask is 255.255.255.0
As we need 6 subnets, we need three extra 1's. Hence, the subnet mask is 255.255.255.224
In a binary form the subnet mask is



In order to have six subnets, we can have 6 different combinations of the 3- extra 1s as shown in table 1.

Table 1

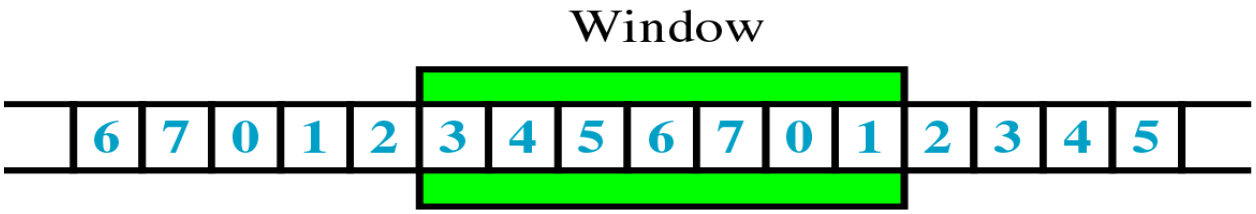
Combination	**Subnet Number**
000	Subnet 1
001	Subnet 2
010	Subnet 3
011	Subnet 4
100	Subnet 5
101	Subnet 6

Therefore, the various addresses of 6 subnets are as shown in table 2.

Table 2

Subnet N0.	**Addresses**
1	201.70.64.0 to 201.70.64.31
2	201.70.64.32 to 201.70.64.63
3	201.70.64.64 to 201.70.64.95
4	201.70.64.96 to 201.70.64.127
5	201.70.64.128 to 201.70.64.159
6	201.70.64.160 to 201.70.64.191

(b) The sender can send transmit several frames before needing an acknowledgement. The receiver acknowledges only some of the frames, using a single ACK to confirm the receipt of multiple data frames.



- Sliding window: refers to imaginary boxes at both the sender and receiver.
- Frames may be ACK'ed at any point without waiting for the window to fill up and may be transmitted as long as the window is not yet full
- Frames are numbered modulo N: 0, 1, 2, …, N-1
- Window size cannot exceed N-1 → max. number of N-1 frames can be sent before an ACK is required
- An ACK with number K means all frames up thru K-1 have been received.
- **Sender Sliding Window Side**

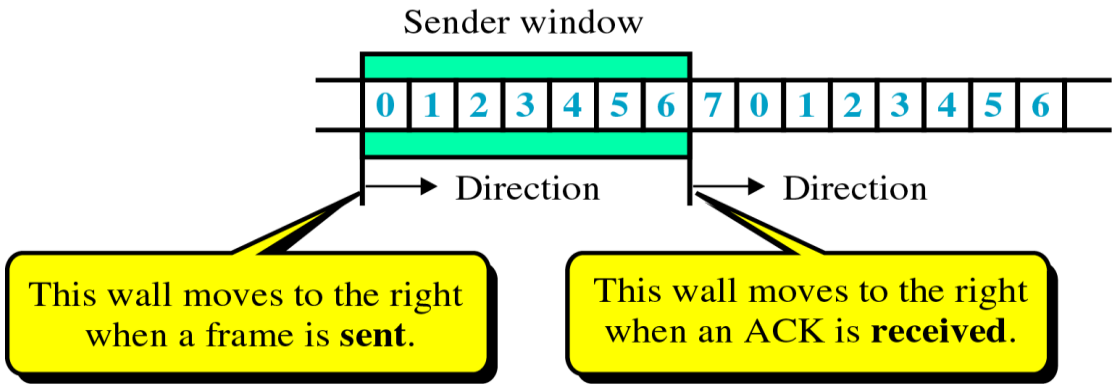


Fig.6 (a): Sender Sliding Window

• At the beginning of a transmission, the sender's window contains n-l frames.
• As the frames are sent by source, the left boundary of the window moves inward, shrinking the size of window.
• When the receiver sends an ACK, the source's window expand i.e. (right boundary moves outward) to allow in a number of new frames equal to the number of frames acknowledged by that ACK.

Receiver Sliding Window

- At the beginning of transmission, the receiver's window contains n-1 spaces for frame but not the frames.

- As the new frames come in, the size of window shrinks.
- Therefore the receiver window represents not the number of frames received but the number of frames that may still be received without an acknowledgment ACK must be sent.
- Given a window of size w, if three frames are received without an ACK being returned, the number of spaces in a window is w-3.
- As soon as acknowledgment is sent, window expands to include the number of frames equal to the number of frames acknowledged.

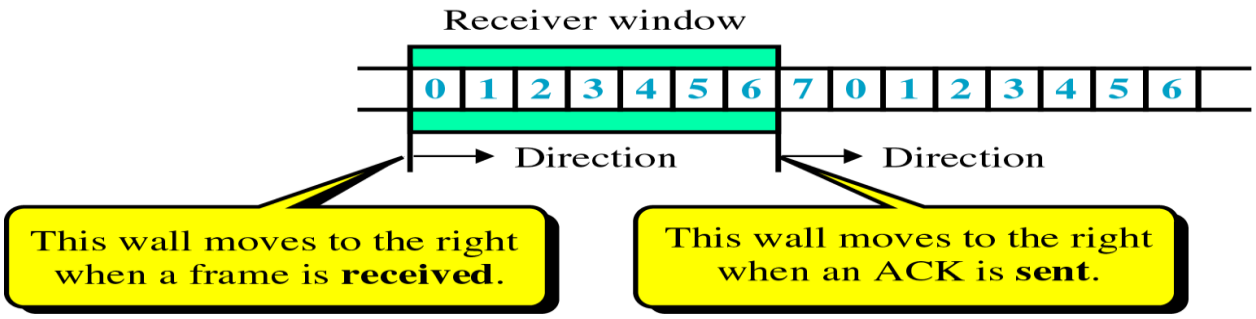


Fig.6 (b): Receiver Sliding Window

Example of Sliding Window

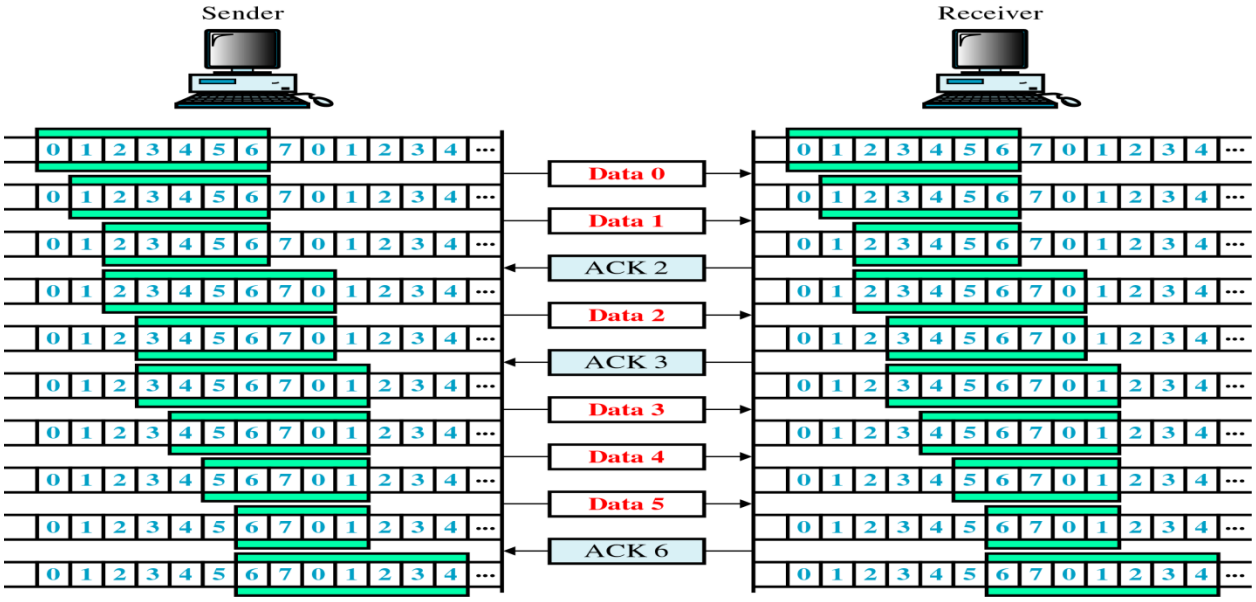
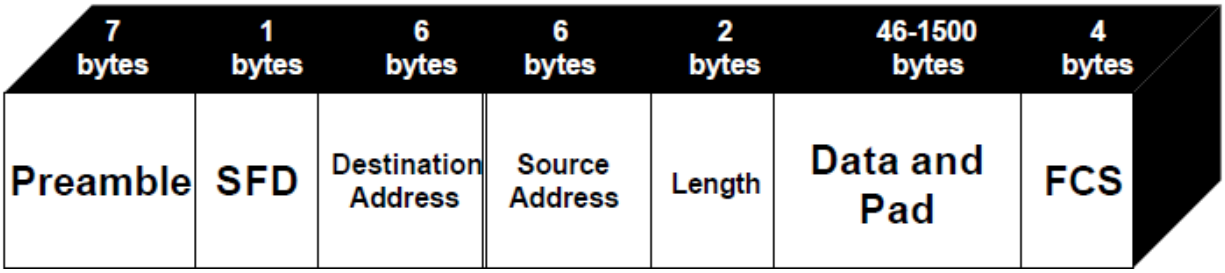


Fig.6 (c): Example of Sliding Window

7(a): IEEE 802.3 Frame Format
The IEEE standard was adopted in 1985. The 802.3 frame format is below:



The Preamble of the frame (the first 7 bytes) indicates the start of a new frame and establishes synchronization conditions between devices.

The Start Frame Delimiter (SFD) has the same 10101011-bit sequence found at the end of the preamble. Both formats use the same number of bytes to perform the synchronization of the signals.

The Destination and Source Addresses can be either 2 or 6 bytes. Whether 2 or 6 bytes are used, all devices within the same network must use the same format. IEEE protocols specify that a 10Mbs network must use 6 bytes. The 2 byte length is obsolete.

The Length field indicates the number of bytes in the data field. If the data field is less than the required 46 bytes, a pad field is added to the data frame. The bytes added for padding purposes are usually zeros.

The data field contains the data to be transmitted from device to device.

The Frame Check Sequence (FCS) field is used as an error detection function. The error detection function is a calculation completed by both the source and destination devices. If the calculations do not match, an error is then generated.

(b)

Table 3:Comparison of Virtual-Circuit and Datagram Networks

Issue	Datagram network	Virtual-circuit network
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

(c) In case of FDMA the bandwidth is divided into separate frequency bands. In case of TDMA the bandwidth is timeshared. On the other hand in case of CDMA data from all stations are transmitted simultaneously and are separated based on coding theory. Unlike FDMA, CDMA has soft capacity, which means that there is no hard limit on the number of users. Capacity of FDMA and TDMA is bandwidth limited, whereas the bandwidth of CDMA is interference limited. CDMA offers high capacity in comparison to FDMA and TDMA. CDMA also help to combat multipath fading.

8(a): A computer network is an interconnection of various computer systems located at different places. In computer network two or more computers are linked together with a medium and data communication devices for the purpose of communicating data and sharing resources. The computer that provides resources to other computers on a network is known as server. In the network the individual computers, which access shared network resources, are known as workstations or nodes.

Computer Networks may be classified on the basis of geographical area in two broad categories.

1. Local Area Network (LAN)

2. Wide Area Network (WAN)

I. Local Area Network:

Networks used to interconnect computers in a single room, rooms within a building or buildings on one site are called Local Area Network (LAN). LAN transmits data with a speed of several megabits per second (106 bits per second). The transmission medium is normally coaxial cables.

LAN links computers, i.e., software and hardware, in the same area for the purpose of sharing information. Usually LAN links computers within a limited geographical area because they must be connected by a cable, which is quite expensive. People working in LAN get more capabilities in data processing, work processing and other information exchange compared to stand-alone computers. Because of this information exchange most of the business and government organizations are using LAN.

Major Characteristics of LAN are as follows:

- *Every computer has the potential to communicate with any other computers of the network*
- *High degree of interconnection between computers*
- *Easy physical connection of computers in a network*
- *Inexpensive medium of data transmission*
- *High data transmission rate*

Advantages of LAN are as follows:

- The reliability of network is high because the failure of one computer in the network does not effect the functioning for other computers.
- Addition of new computer to network is easy.
- High rate of data transmission is possible.
- Peripheral devices like magnetic disk and printer can be shared by other computers.

Disadvantages of LAN is

If the communication line fails, the entire network system breaks down.

Use of LAN

Followings are the major areas where LAN is normally used

- File transfers and Access
- Word and text processing
- Electronic message handling
- Remote database access
- Personal computing
- Digital voice transmission and storage

II. Wide Area Network:

The term Wide Area Network (WAN) is used to describe a computer network spanning a regional, national or global area. For example, for a large company the head quarters might be at Delhi and Regional branches at Bombay, Madras, Bangalore and Calcutta. Here regional centers are connected to head quarters through WAN. The distance between computers connected to WAN is larger. Therefore the transmission medium used is normally telephone lines, microwaves and satellite links.

Characteristics of WAN are as follows:

a. *Communication Facility:* For a big company spanning over different parts of the country the employees can save long distance phone calls and it overcomes the time lag in overseas

communications. Computer conferencing is another use of WAN where users communicate with each other through their computer system.

b. *Remote Data Entry:* Remote data entry is possible in WAN. It means sitting at any location you can enter data, update data and query other information of any computer attached to the WAN but located in other cities. For example, suppose you are sitting at Madras and want to see some data of a computer located at Delhi, you can do it through WAN.

c. *Centralized Information:* In modern computerized environment you will find that big organizations go for centralized data storage. This means if the organization is spread over many cities, they keep their important business data in a single place. As the data are generated at different sites, WAN permits collection of this data from different sites and save at a single site.

Examples of WAN are as follows:

a. *Ethernet:* Ethernet developed by Xerox Corporation is a famous example of WAN. This network uses coaxial cables for data transmission. Special integrated circuit chips called controllers are used to connect equipment to the cable.

b. *Arpanet:* The Arpanet is another example of WAN. It was developed at Advanced Research Projects Agency of U. S. Department. This Network connects more than 40 universities and institutions throughout USA and Europe.

Difference between LAN and WAN are as follows:

- LAN is restricted to limited geographical area of few kilometers. But WAN covers great distance and operate nationwide or even worldwide.
- In LAN, the computer terminals and peripheral devices are connected with wires and coaxial cables. In WAN there is no physical connection. Communication is done through telephone lines and satellite links.
- Cost of data transmission in LAN is less because the transmission medium is owned by a single organization. In case of WAN the cost of data transmission is very high because the transmission medium used is hired either telephone lines or satellite links.
- The speed of data transmission is much higher in LAN than in WAN. The transmission speed in LAN varies from 0.1 to 100 megabits per second. In case of WAN the speed ranges from 1800 to 9600 bits per second (bps).
- Few data transmission errors occur in LAN compared to WAN. It is because in LAN the distance covered is negligible.

III. Hybrid Networks:

Between the LAN and WAN structures, you will find hybrid networks such as campus area networks (CANs) and metropolitan area networks (MANs). In addition, a new form of network type is emerging called home area networks (HANs). The need to access corporate Web sites has created two classifications known as intranets and extranets. The following sections introduce these networks.

a. Campus Area Networks (CANs): A campus area network (CAN) follows the same principles as a local area network, only on a larger and more diversified scale. With a CAN, different campus offices and organizations can be linked together. For example, in a typical

university setting, accounts office might be linked to a registrar's office. In this manner, once a student has paid his or her tuition fees in the accounts section, this information is transmitted to the registrar's system so the student can enroll for classes. Some university departments or organizations might be linked to the CAN even though they already have their own separate LANs.

b. Metropolitan Area Networks (MANs): The metropolitan area network (MAN) is a large-scale network that connects multiple corporate LANs together. MANs usually are not owned by a single organization; their communication devices and equipment arc usually maintained by a group or single network provider that sells its networking services to corporate customers. MANs often take the role of a high-speed network that allows for the sharing of regional resources. MANs also can provide a shared connection to other networks using a WAN link.

c. Home Area Networks (HANs): A home area network (HAN) is a network contained within a user's home connects a person's digital devices, from multiple computers and their peripheral devices, such as a printer, to telephones, VCRs, DVDs, televisions, video games, between LANs, MANs. Home security systems, "smart" appliances, fax machines, and other digital devices that are wired into the network.

d. Intranets and Extranets: Much of the technology available on the Internet is also available for private network use. The company's internal version of the Internet is called an intranet. An intranet uses the same Web server software that gives the public access to Web sites over the Internet. The major difference is that an intranet usually limits access to employees and selected contractors having ongoing business with the company.

(b) Token Ring Operation:

Token-passing networks move a small frame, called a token, around the network. Possession of the token grants the right to transmit. If a node receiving the token has no information to send, it passes the token to the next end station. Each station can hold the token for a maximum period of time.

If a station possessing the token does have information to transmit, it seizes the token, alters 1 bit of the token (which turns the token into a start-of-frame sequence), appends the information that it wants to transmit, and sends this information to the next station on the ring. While the information frame is circling the ring, no token is on the network (unless the ring supports early token release), which means that other stations wanting to transmit must wait. Therefore, collisions cannot occur in Token Ring networks. If early token release is supported, a new token can be released immediately after a frame transmission is complete. The information frame circulates around the ring until it reaches the intended destination station, which copies the information for further processing. The information frame makes a round trip and is finally removed when it reaches the sending station. The sending station can check the returning frame to see whether the frame was seen and subsequently copied by the destination station in error-free form. Then the sending station inserts a new free token on the ring, if it has finished transmission of its packets. Unlike CSMA/CD networks (such as Ethernet), token-passing networks are deterministic, which means that it is possible to calculate the maximum time that

will pass before any end station will be capable of transmitting. Token Ring networks are ideal for applications in which delay must be predictable and robust network operation is important.

9(a): Functions of a Token Bus

It is the technique in which the station on bus or tree forms a logical ring that is the stations are assigned positions in an ordered sequence, with the last number of the sequence followed by the first one as shown in Fig. Each station knows the identity of the station following it and preceding it.

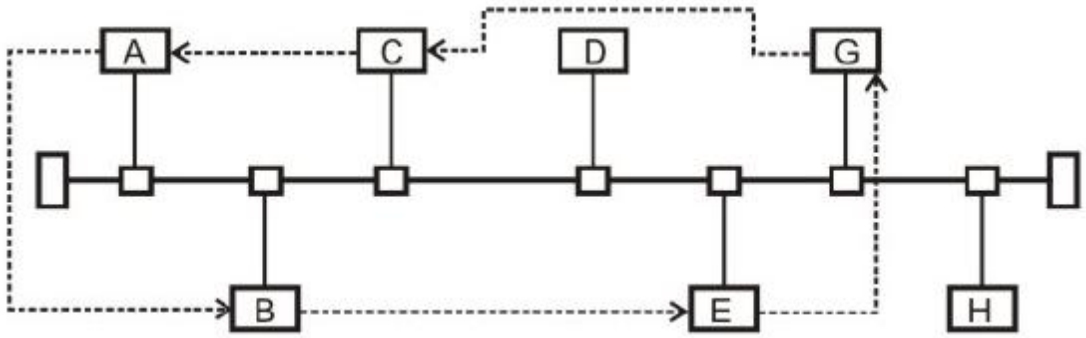


Fig.9 (a): Token Bus

A control packet known as a Token regulates the right to access. When a station receives the token, it is granted control to the media for a specified time, during which it may transmit one or more packets and may poll stations and receive responses when the station is done, or if its time has expired then it passes token to next station in logical sequence. Hence, steady phase consists of alternate phases of token passing and data transfer.

(b)Advantage of token passing protocol over CSMA/CD protocol:

The CSMA/CD is not a deterministic protocol. A packet may be delivered after many (up to 15) collisions leading to long variable delay. An unfortunate packet may not get delivered at all. This feature makes CSMA/CD protocol unsuitable for real-time applications. On the other hand, token passing protocol is a deterministic approach, which allows a packet to be delivered within a known time frame. It also allows priority to be assigned to packets. These are the two key advantages of token passing protocol over CSMA/CD protocol.

(c) Token ring protocol cannot work if a link or a station fails. So, it is vulnerable to link and station failure.

(d) Token ring is maintained with the help of active token monitor. Any one of the stations has the capability to act as active token monitor, but at a particular instant only one acts as active token monitor. It monitors various error situations such as multiple token, orphan packet, etc, and takes appropriate action to come out of the error situation.