

Networking Technology for Digital Devices

Q.1 a] what is CRC? Write the algorithm for computing checksum and explain with suitable example. (10 Marks)

Ans:-

CRC: - Cyclic Redundancy Check is cyclic codes to correct errors.

Checksum:-

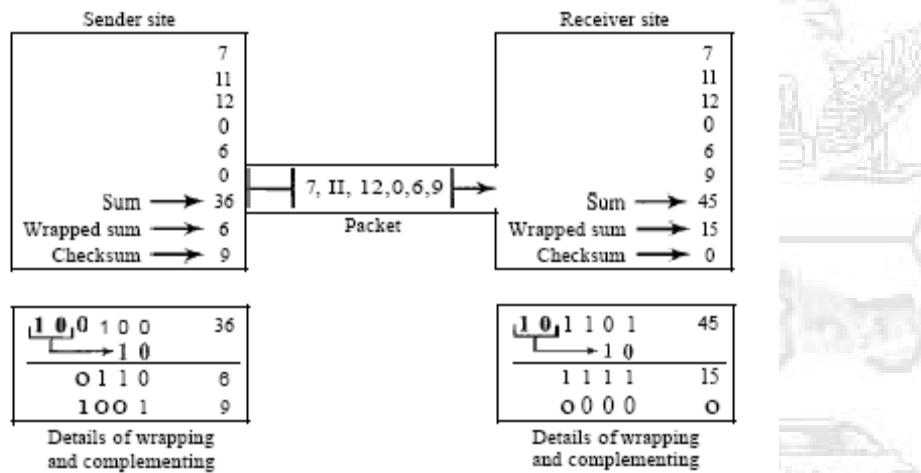
Sender site:

1. The message is divided into 16-bit words.
2. The value of the checksum word is set to 0.
3. All words including the checksum are added using one's complement addition.
4. The sum is complemented and becomes the checksum.
5. The checksum is sent with the data.

Receiver site:

1. The message (including checksum) is divided into 16-bit words.
2. All words are added using one's complement addition.
3. The sum is complemented and becomes the new checksum.
4. If the value of checksum is 0, the message is accepted; otherwise, it is rejected.

Example:-

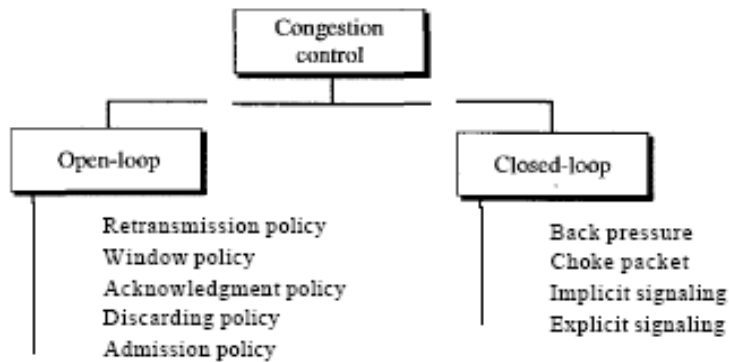


Q.1 b] Explain how TCP controls congestion. (10 Marks)

Ans:-

Congestion in a network may occur if the load on the network-the number of packets sent to the network-is greater than the capacity of the network-the number of packets a network can handle. Congestion control refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.

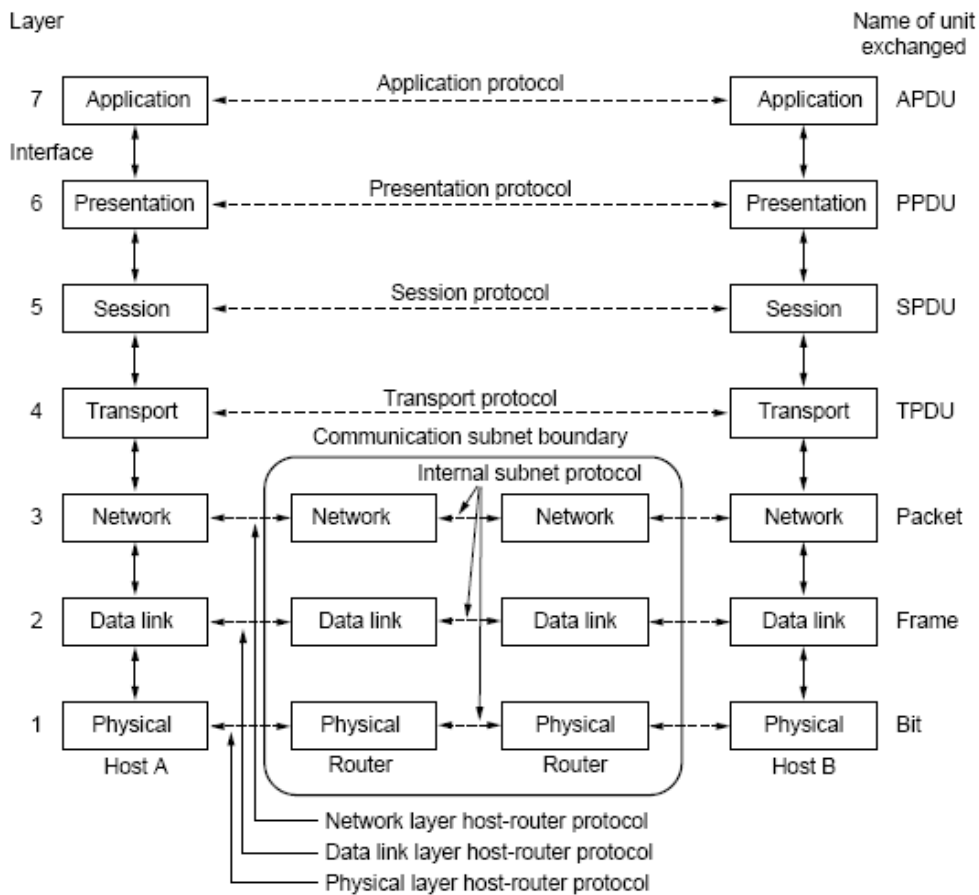
Networking Technology for Digital Devices



1. Leaky Bucket
2. Token Bucket

Q.2 a] Explain ISO OSI reference model in detail. (10 Marks)

Ans:



Physical Layer:-

1. Representation of bit
2. Data rate
3. Physical topology

Networking Technology for Digital Devices

4. Line configuration

Data link Layer:-

1. Framing
2. Flow control
3. Error control
4. Access control

Network Layer:-

1. Logical addressing
2. Routing

Transport Layer:-

1. Connection control
2. Segmentation and reassembly
3. Service point addressing

Session Layer:-

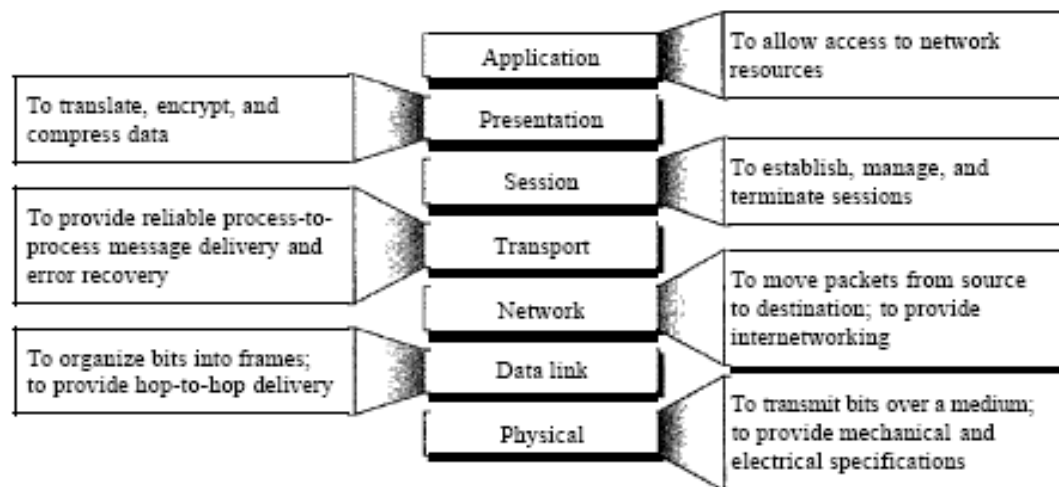
1. Dialog control
2. Synchronization

Presentation Layer:-

1. Translation
2. Encryption
3. Compression

Application Layer:-

1. File transfer access and management
2. Mail service



Q.2 b] what is buffering? Explain different types of buffering. (10 Marks)

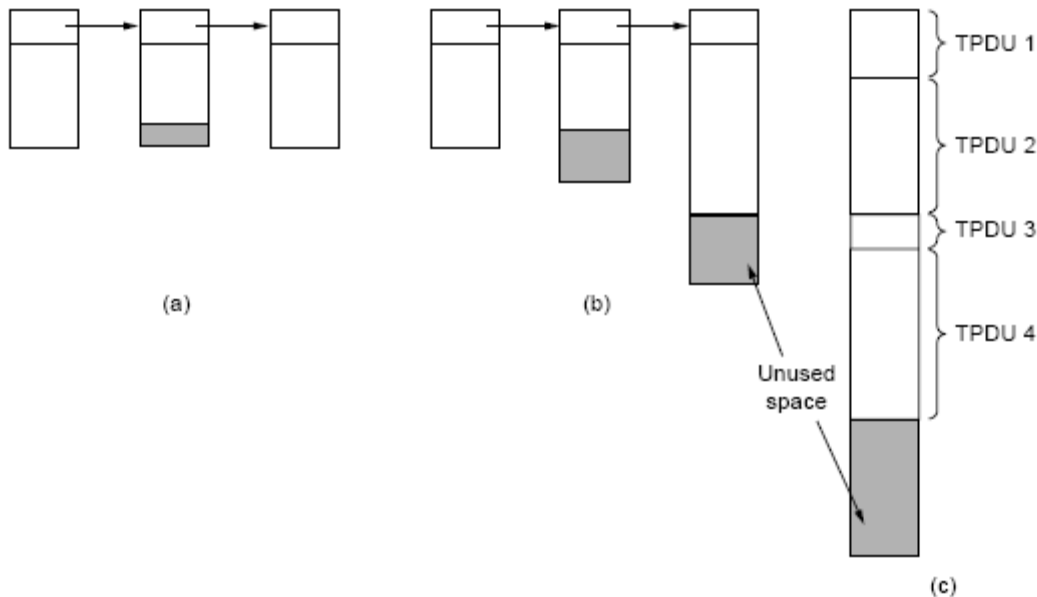
Ans: -

Buffering is storage where frame are store.

Types

1. Chained fixed-size buffer

2. Chained variable-size buffer
3. One large circular buffer per connection



(a) Chained fixed-size buffers. (b) Chained variablesized buffers. (c) One large circular buffer per connection.

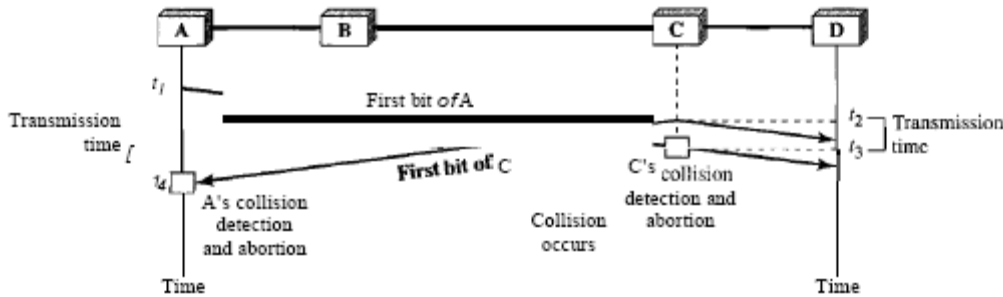
Q.3 a] Explain CSMA/CD. (10 Marks)

Ans

carrier sense multiple access with collision detection (CSMA/CD) An access method in which stations transmit whenever the transmission medium is available and retransmit when collision occurs. In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, however, there is a collision, the frame is sent again. To better understand CSMA/CD, let us look at the first bits transmitted by the two stations involved in the collision. Although each station continues to send bits in the frame until it detects the collision, we show what happens as the first bits collide. In Figure stations A and C are involved in the collision. At time t_1 , station A has executed its persistence procedure and starts sending the bits of its frame. At time t_2 , station C has not yet sensed the first bit sent by A. Station C executes its persistence procedure and starts sending the bits in its frame, which propagate both to the left and to the right. The collision occurs sometime after time t_2' Station C detects a collision at time t_3 when it receives the first bit of A's frame. Station C immediately (or after a short time, but we assume immediately) aborts transmission. Station A detects collision at time t_4 when it receives the first bit of C's frame; it also immediately aborts transmission. Looking at the figure, we see that A transmits for the duration $t_4 - t_1$; C transmits for the duration $t_3 - t_2'$ Later we show that, for the

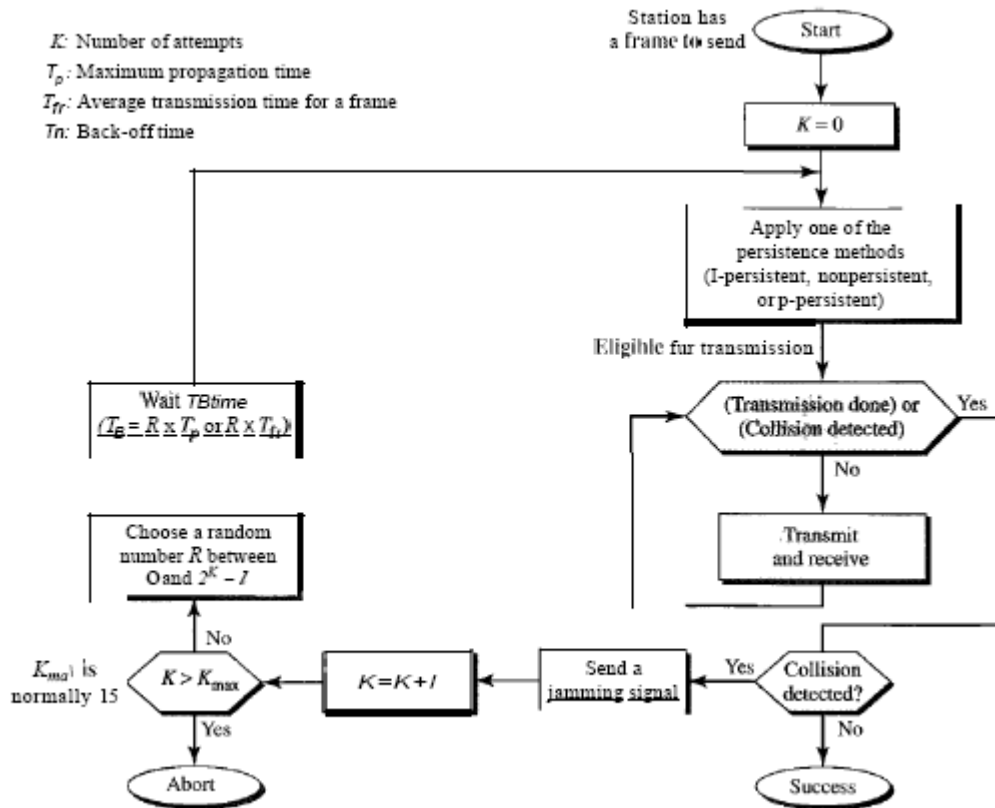
Networking Technology for Digital Devices

protocol to work, the length of any frame divided by the bit rate in this protocol must be more than either of these durations. At time t_4 , the transmission of A's frame, though incomplete, is aborted; at time t_3 , the transmission of B's frame, though incomplete, is aborted.



Procedure

Now let us look at the flow diagram for CSMA/CD in Figure It is similar to the one for the ALOHA protocol, but there are differences. The first difference is the addition of the persistence process. We need to sense the channel before we start sending the frame by using one of the persistence processes (nonpersistent, I-persistent, or p-persistent). The corresponding box can be replaced by one of the persistence processes shown in Figure The second difference is the frame transmission. In ALOHA, we first transmit the entire frame and then wait for an acknowledgment. In CSMA/CD, transmission and collision detection is a continuous process. We do not send the entire frame and then look for a collision. The station transmits and receives continuously and simultaneously (using two different ports). We use a loop to show that transmission is a continuous process. We constantly monitor in order to detect one of two conditions: either transmission is finished or a collision is detected. Either event stops transmission. When we come out of the loop, if a collision has not been detected, it means that transmission is complete; the entire frame is transmitted. Otherwise, a collision has occurred. The third difference is the sending of a short jamming signal that enforces the collision in case other stations have not yet sensed the collision.



Q.3 b] Explain different distributed computing model with example. (10 Marks)

Ans:-

1. Minicomputer
2. Workstation
3. Workstation-server
4. Processor-pool
5. Hybrid

Minicomputer:-

Simple extension of the centralized time-sharing system Example-ARPAnet

Workstation:-

Each workstation equipped with its own disk and serving as single user computer. Example:- organization, office, college etc.

Workstation-server:-

Consist of few minicomputer and several workstations. Example Vsystem.

Processor Pool:-

Based on the observation that most of the time a user does not need any computing power but once in a while he or she may need a very large amount of computing power for short time. Example

Networking Technology for Digital Devices

when recompiling a program consisting of a large numbers of files after changing basic shared declaration.

Hybrid :-

Combination of model.

Q.4 a] Explain various issues in networking security. (10 Marks)

Ans:- Requirement of network security 2 Marks

*Each issues carries 2 Marks (04*02=08)*

Network Security issues:-

Secrecy

Authentication

Non repudiation

Integrity

Network security problems can be divided roughly into four closely intertwined areas: secrecy, authentication, non repudiation, and integrity control. Secrecy, also called confidentiality, has to do with keeping information out of the hands of unauthorized users. This is what usually comes to mind when people think about network security. Authentication deals with determining whom you are talking to before revealing sensitive information or entering into a business deal. Nonrepudiation deals with signatures: How do you prove that your customer really placed an electronic order for ten million left-handed doohickeys at 89 cents each when he later claims the price was 69 cents? Or maybe he claims he never placed any order. Finally, how can you be sure that a message you received was really the one sent and not something that a malicious adversary modified in transit or concocted?

Q.4 b] what is internetworking? Describe the devices used in the internetworking. (10 Marks)

Ans:-

Internetworking:-

Internetworking is the practice of connecting a computer network with other networks through the use of gateways that provide a common method of routing information packets between the networks. The resulting system of interconnected networks is called an internet work, or simply an internet.

OR

One or more connected LANs.

Devices:-

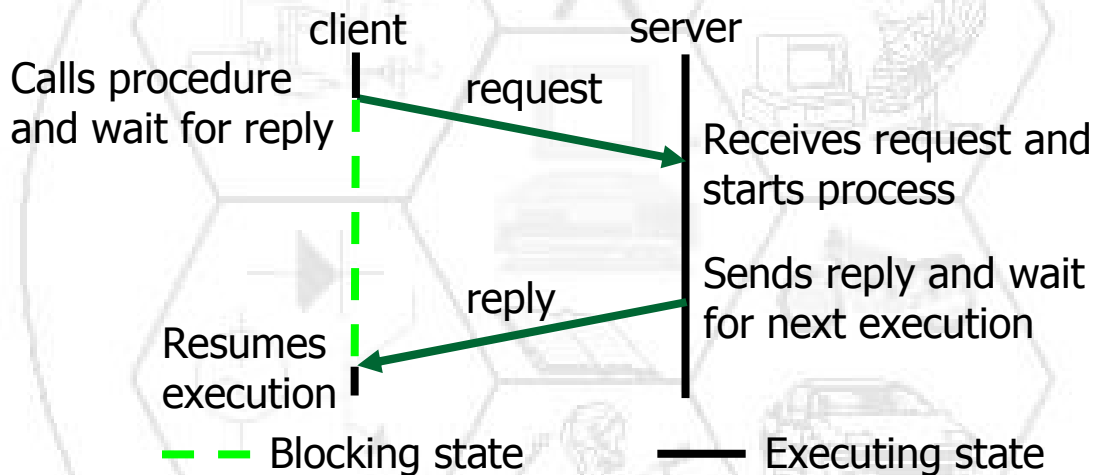
Networking Technology for Digital Devices

1. Hub
2. Switch
3. Router
4. Gateway
5. NIC
6. Bridge

Q.5 a] Explain Remote Procedure Call. (10 Marks)

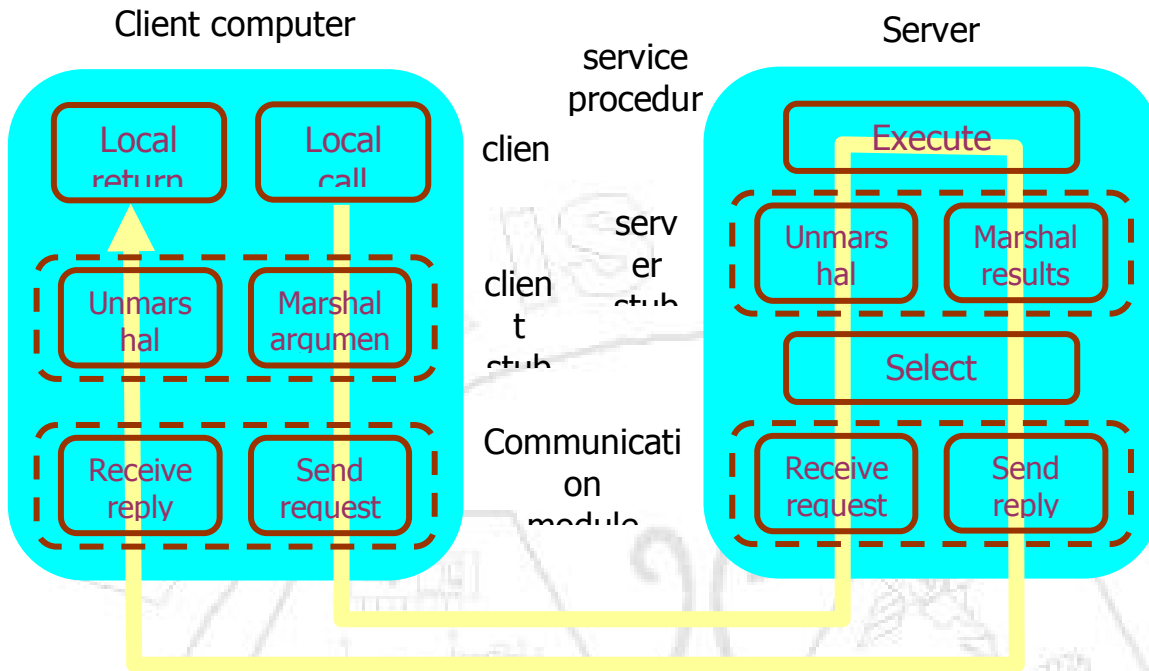
Ans:-

- Remote Procedure Call (RPC) is a high-level model for client-server communication.
- RPC enables clients to communicate with servers by calling procedures in a similar way to the conventional use of procedure calls in high-level languages.
- Examples: File service, Authentication service.



- The client transfer call request (the procedure name) and the arguments to the server via client stub function
- stub function
 - marshals arguments and places them into a message together with the remote procedure identifier.
 - Sends message to server and waits for call return
- Server receives the call request and passes to an appropriate server stub function.
- 6. server stub function unmarshals the arguments, call the corresponding (local) service procedure.
- On return, the server stub marshals the output arguments into a call return message and sends back to the client.

- Client stub receives call reply, unmarshals value, returns to client code



Q.5 b) Explain how the failure handling is done. (10 Marks)

Ans:-

Loss request message:-

This may happen either due to the failure of communication link between sender and receiver or because the receiver node is down at the time the request message reaches there.

Loss of response message:-

This may happen either due to the failure of communication link between the sender and receiver or because the senders node is down at the time the response message reaches there.

Unsuccessful execution of the request:-

This happens due to the receivers node crashing while the request is being processed.

Q.6 a) what is Multiplexing? Explain different types of multiplexing. (10 Marks)

Ans:-

Multiplexing:-

In telecommunications and computer networks, multiplexing (also known as muxing) is a process where multiple analog message signals or digital data streams are combined into one signal over a shared medium.

Types:-

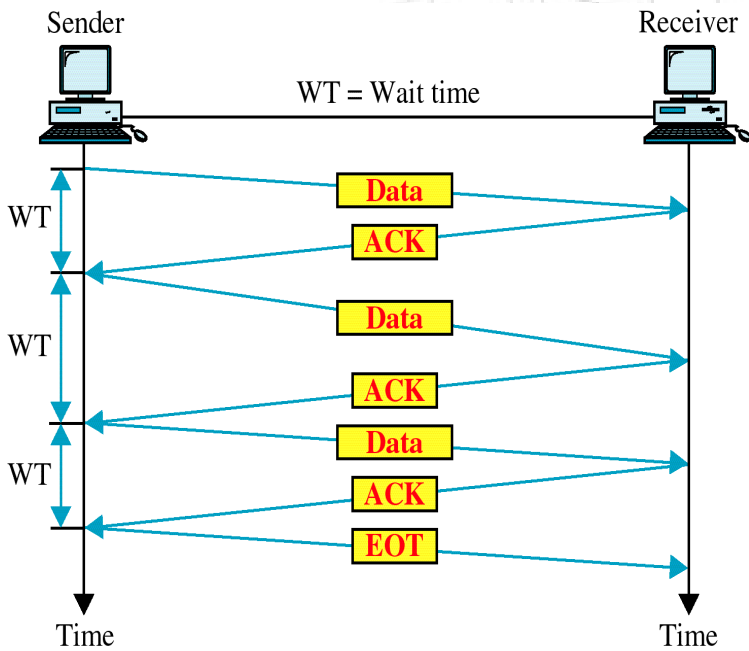
1. TDM
2. FDM

3. WDM

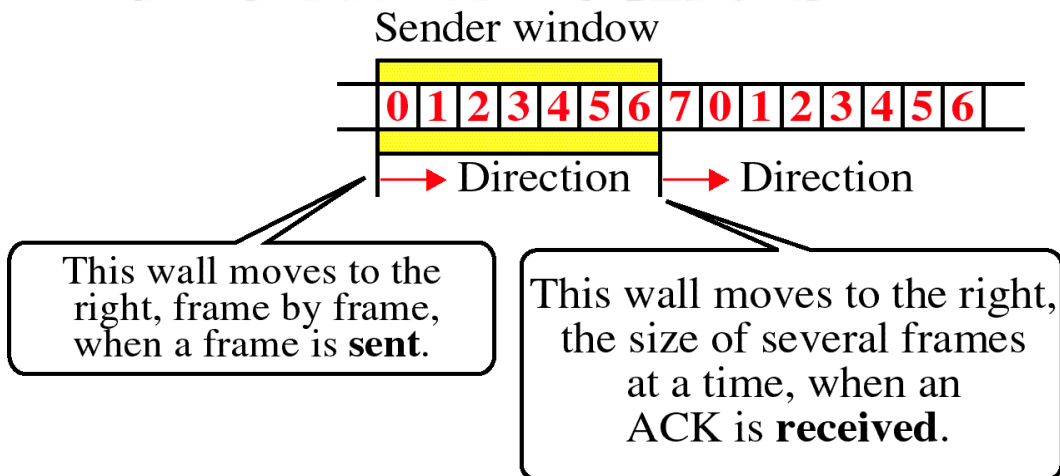
Q.6 b] Explain Stop and wait protocol and Sliding window protocol. (10 Marks)

Ans:-

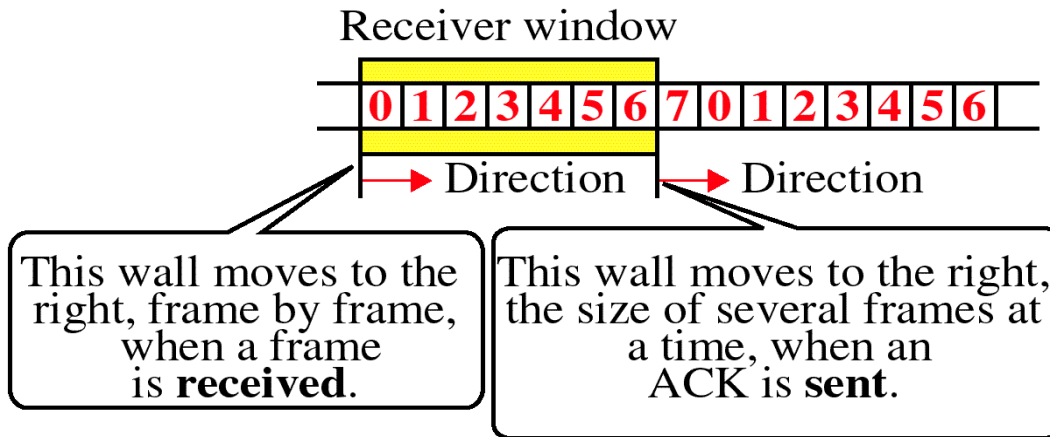
Stop and Wait Protocol:-



Sliding window protocol:-



Receiver Sliding Window



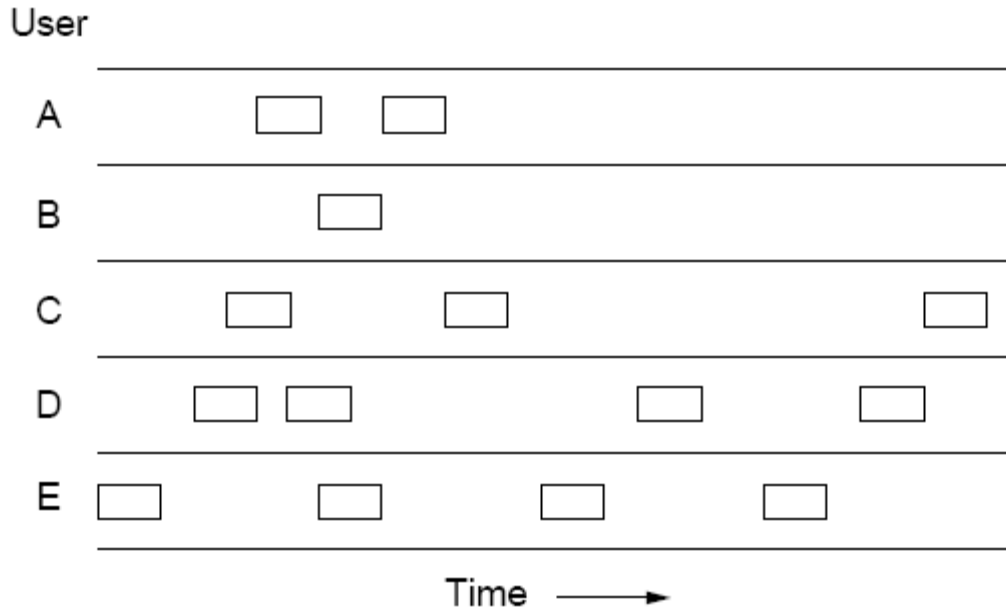
Q.7 Write short notes on :- (20 Marks) Each note carries 05 Marks

a) ALOHA

Ans:-

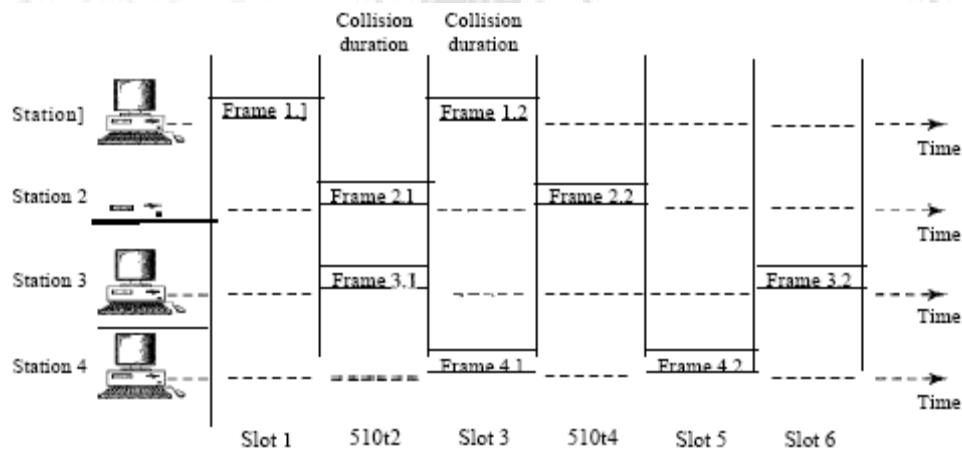
Pure ALOHA

The basic idea of an ALOHA system is simple: let users transmit whenever they have data to be sent. There will be collisions, of course, and the colliding frames will be damaged. However, due to the feedback property of broadcasting, a sender can always find out whether its frame was destroyed by listening to the channel, the same way other users do. With a LAN, the feedback is immediate; with a satellite, there is a delay of 270 msec before the sender knows if the transmission was successful. If listening while transmitting is not possible for some reason, acknowledgements are needed. If the frame was destroyed, the sender just waits a random amount of time and sends it again. The waiting time must be random or the same frames will collide over and over, in lockstep. Systems in which multiple users share a common channel in a way that can lead to conflicts are widely known as contention systems.



Slotted ALOHA

In 1972, Roberts published a method for doubling the capacity of an ALOHA system (Roberts, 1972). His proposal was to divide time into discrete intervals, each interval corresponding to one frame. This approach requires the users to agree on slot boundaries. One way to achieve synchronization would be to have one special station emit a pip at the start of each interval, like a clock. In Roberts' method, which has come to be known as slotted ALOHA, in contrast to Abramson's pure ALOHA, a computer is not permitted to send whenever a carriage return is typed. Instead, it is required to wait for the beginning of the next slot. Thus, the continuous pure ALOHA is turned into a discrete one.



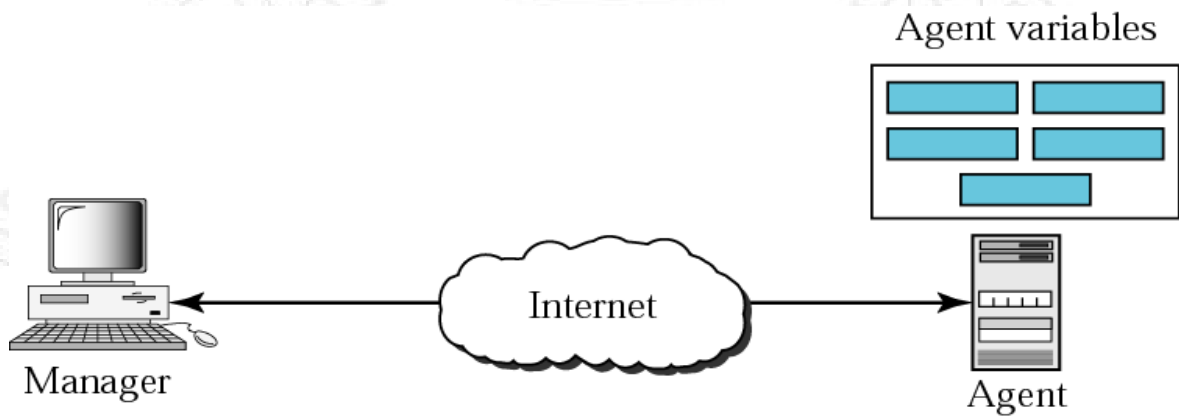
b] **SNMP:-**

Ans:-

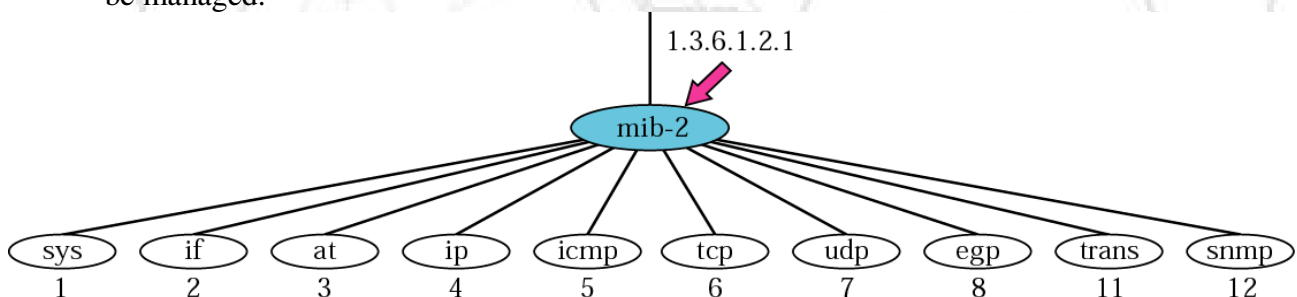
Manager agent

SMI

MIB



SNMP defines the format of packets exchanged between a manager and an agent. It reads and changes the status (values) of objects (variables) in SNMP packets. SMI defines the general rules for naming objects, defining object types (including range and length), and showing how to encode objects and values. SMI defines neither the number of objects an entity should manage, nor names the objects to be managed nor defines the association between the objects and their values. MIB creates a collection of named objects, their types, and their relationships to each other in an entity to be managed.



c] **ARP, RARP**

Ans:-

Address Resolution Protocol

Networking Technology for Digital Devices

The Address Resolution Protocol (ARP) is used to associate a logical address with a physical address. On a typical physical network, such as a LAN, each device on a link is identified by a physical or station address, usually imprinted on the network interface card (NIC). ARP is used to find the physical address of the node when its Internet address is known.

Reverse Address Resolution Protocol

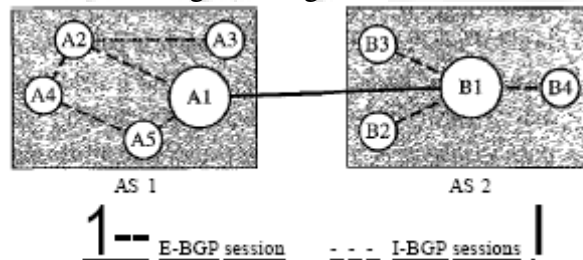
The Reverse Address Resolution Protocol (RARP) allows a host to discover its Internet address when it knows only its physical address. It is used when a computer is connected to a network for the first time or when a diskless computer is booted.

d] **BGP:-**

Ans

BGP

Border Gateway Protocol (BGP) is an interdomain routing protocol using path vector routing. It first appeared in 1989 and has gone through four versions. BGP Sessions The exchange of routing information between two routers using BGP takes place in a session. A session is a connection that is established between two BGP routers only for the sake of exchanging routing information. To create a reliable environment, BGP uses the services of TCP. In other words, a session at the BGP level, as an application program, is a connection at the TCP level. However, there is a subtle difference between a connection in TCP made for BGP and other application programs. When a TCP connection is created for BGP, it can last for a long time, until something unusual happens. For this reason, BGP sessions are sometimes referred to as semipermanent connections. External and Internal BGP If we want to be precise, BGP can have two types of sessions: external BGP (E-BGP) and internal BGP (I-BGP) sessions. The E-BGP session is used to exchange information between two speaker nodes belonging to two different autonomous systems. The I-BGP session, on the other hand, is used to exchange routing information between two routers inside an autonomous system.



References:-

1. A.S.Tanenbaum, "Computer Networks", Pearson Education, Fourth Edition.
2. Data Communication And Networking 4th Edition by B.A. Forouzan Tata McGrawhill Publication.
3. Distributed Operating Systems, P. K. Sinha, IEEE Press

