Solution:- T1624 - S.E.(INFORMATION TECHNOLOGY)(SEM IV)(REV-2012) (CBSGS) / T1078 - COMPUTER NETWORKS Q.Paper code : 13124

Q.1. a) **1. Services provided to the network layer:**

A well-defined service interface to the network layer on source machine to the network layer on destination machine.

2. Frame synchronisation: The source machine sends data in blocks called frames to the destination machine. The starting and ending of each frame should be recognised by the destination machine.

3. Flow control The source machine must not send data frames at a rate faster than the destination machine can accept them.

4. Error control: The errors made in bits during transmission from source to destination machines must be detected and corrected.

5. Addressing: On a multipoint line, such as many machines connected together (LAN), the identity of the individual machines must be specified while transmitting the data frames.

6. Control and data on same link: The data and control information is combined in a frame and transmitted from the source to destination machine. The destination machine must be able to recognise control information from the data being transmitted.

7. Link Management: The initiation, maintenance and termination of the link between the source and destination are required for effective exchange of data. It requires co-ordination and co-operation among stations. Protocols or procedures are required for the link management.

Q1.b)

An IP address, short for Internet Protocol address, is an identifying number for a piece of network hardware. Having an IP address allows a device to communicate with other devices over an IP-based network like the internet. Most IP addresses look like this:151.101.65.121

Every NIC has a hardware address that's known as a MAC, for Media Access Control. Where IP addresses are associated with TCP/IP (networking software), MAC addresses are linked to the hardware of network adapters. A MAC address is given to a network adapter when it is manufactured. It is hardwired or hard-coded onto your computer's network interface card (NIC) and is unique to it.

Port Address:Port address is a feature of a network device that translates TCP or UDP communications made between a host and port on an outside network It allows a single IP address to be used for many internal hosts. Port address can automatically modify the IP packets' destination or source host IP and port fields belonging to its internal hosts.

Q.1 c) An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e. Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x. Class B has 16384 (214) Network addresses and 65534 (216-2) Host addresses.

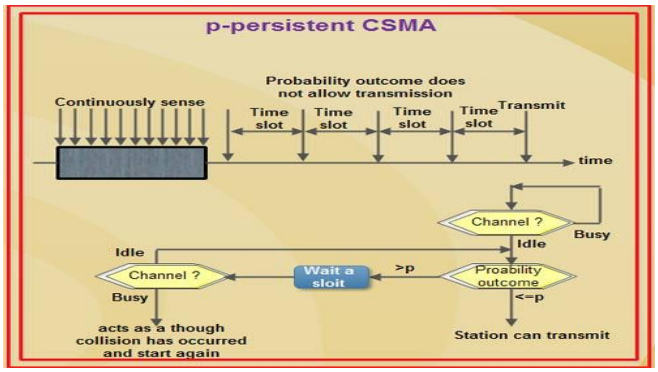
A Subnet mask is a 32-bit number that masks an IP address, and divides the IP address into network address and host address. Subnet Mask is made by setting network bits to all "1"s and setting host bits to all "0"s. Within a given network, two host addresses are reserved for special purpose, and cannot be assigned to hosts. The "0" address is assigned a network address and "255" is assigned to a broadcast address, and they cannot be assigned to hosts

Q.1 d) Atleast 5 points of difference in terms of price, easy of use, security, software, hardware,reliability etc. need to be specified each carrying

Q.1 e) p-persistent CSMA:- This method is used when channel has time slots such that the time slot duration is equal to or greater than the maximum propagation delay time.

• Whenever a station becomes ready to send, it senses the channel.• If channel is busy, station waits until next slot. • If channel is idle, it transmits with a probability p.

• With the probability q=l-p, the station then waits for the beginning of the next time slot.• If the next slot is also idle, it either transmits or waits again with probabilities p and q.• This process is repeated till either frame has been transmitted or another station has begun transmitting. • In case of the transmission by another station, the station acts as though a collision has occurred and it waits a random amount of time and starts again.



Q.1 e)

In circuit switching there are 3 phases i) Connection Establishment. ii) Data Transfer.

iii) Connection Released.In Packet switching directly data transfer takes place .

In circuit switching, each data unit know the entire path address which is provided by the source. In Packet switching, each data unit just know the final destination address intermediate path is decided by the routers.

In Circuit switching, data is processed at source system only. In Packet switching, data is processed at all intermediate node including source system.

Delay between data units in circuit switching is uniform. Delay between data units in packet switching is not uniform.

Resource reservation is the feature of circuit switching because path is fixed for data transmission. There is no resource reservation because bandwidth is shared among users.

Circuit switching is more reliable. Packet switching is less reliable.

Wastage of resources are more in Circuit Switching Less wastage of resources as compared to Circuit Switching

Q. 2 a)

Frame Format:

Each frame in HDLC may contain up to six fields, as shown in Figure: a beginning flag field, an address field, a control field, an information field, a frame check sequence (FCS) field, and an ending flag field. In multiple-frame transmissions, the ending flag of one frame can serve as the beginning flag of the next frame.

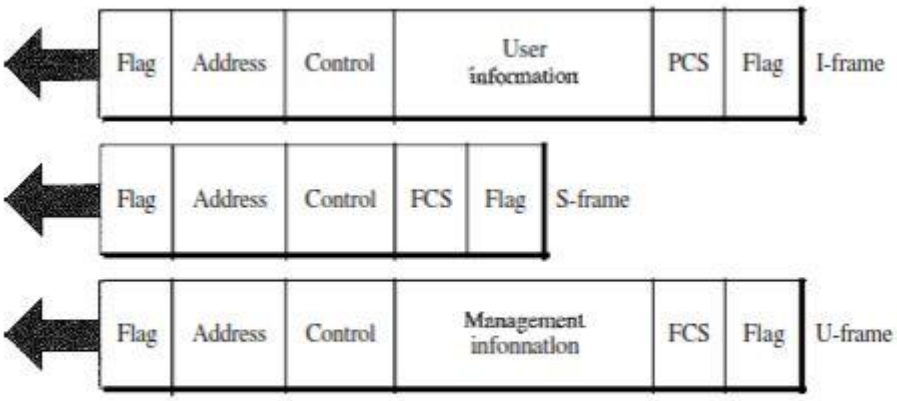


Fig no.29

Flag field: The flag field of an HDLC frame is an 8-bit sequence with the bit pattern 01111110 that identifies both the beginning and the end of a frame and serves as a synchronization pattern for the receiver.

Address field: The second field of an HDLC frame contains the address of the secondary station. If a primary station created the frame, it contains a to address. If a secondary creates the frame, it contains a from address. An address field can be 1 byte or several bytes long, depending on the needs of the network. One byte can identify up to 128 stations (l bit is used for another purpose). Larger networks require multiple-byte address fields. If the address field is only 1 byte, the last bit is always a 1. If the address is more than 1 byte, all bytes but the last one will end with 0; only the last will end with

1. Ending each intermediate byte with 0 indicates to the receiver that there are more address bytes to come.

Control field: The control field is a 1- or 2-byte segment of the frame used for flow and error control. The interpretation of bits in this field depends on the frame type. Information field: The information field contains the user's data from the network layer or management information. Its length can vary from one network to another.

FCS field: The frame check sequence (FCS) is the HDLC error detection field. It can contain either a 2- or 4-byte ITU-T CRC.

Control Field The control field determines the type of frame and defines its functionality. So let us discuss the format of this field in greater detail. The format is specific for the type of frame, as shown in Figure

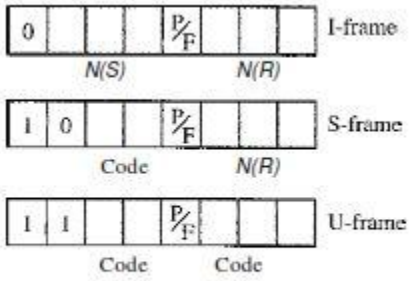


Fig no.30

Control Field for I-Frames:- I-frames are designed to carry user data from the network layer. In addition, they can include flow and error control information (piggybacking). The subfields in the control field are used to define these functions. The first bit defines the type. If the first bit of the control field is 0, this means the frame is an I-frame. The next 3 bits, called N(S), define the sequence number of the frame. Note that with 3 bits, we can define a sequence number between °and 7; but in the extension format, in which the control field is 2 bytes, this field is larger. The last 3 bits, called N(R), correspond to the acknowledgment number when piggybacking is used. The single bit between N(S) and N(R) is called the PIF bit. The PIP field is a single bit with a dual purpose. It has meaning only when it is set (bit = 1) and can mean poll or final. It means poll when the frame is sent by a primary station to a secondary (when the address field contains the address of the receiver). It means final when the frame is sent by a secondary to a primary (when the address field contains the address of the sender).

Control Fieldfor S-Frames Supervisory frames are used for flow and error control whenever piggybacking is either impossible or inappropriate (e.g., when the station either has no data of its own to send or needs to send a command or response other than an acknowledgment). S-frames do not have information fields. If the first 2 bits of the control field is 10, this means the frame is an S-frame. The last 3 bits, called N(R), corresponds to the acknowledgment number (ACK) or negative acknowledgment number (NAK) depending on the type of S-frame. The 2 bits called code is used to define the type of S-frame itself. With 2 bits, we can have four types of S-frames, as described below:

Receive ready (RR): If the value of the code subfield is 00, it is an RR S-frame. This kind of frame acknowledges the receipt of a safe and sound frame or group of frames. In this case, the value N(R) field defines the acknowledgment number. Receive not ready (RNR): If the value of the code subfield is 10, it is an RNR S-frame. This kind of frame is an RR frame with additional functions. It acknowledges the receipt of a frame or group of frames, and it announces that the receiver is busy and cannot receive more frames. It acts as a kind of congestion control mechanism by asking the sender to slow down. The value of N(R) is the acknowledgment number.

Reject (REJ): If the value of the code subfield is 01, it is a REJ S-frame. This is a NAK frame, but not like the one used for Selective Repeat ARQ. It is a NAK that can be used in Go-Back-N ARQ to improve the efficiency of the process by informing the sender, before the sender time expires, that the last frame is lost or damaged. The value of NCR) is the negative acknowledgment number.

Selective reject (SREJ): If the value of the code subfield is 11, it is an SREJ S-frame. This is a NAK frame used in Selective Repeat ARQ. Note that the HDLC Protocol uses the term selective reject instead of selective repeat. The value of N(R) is the negative acknowledgment number.

Control Field for V-Frames Unnumbered frames are used to exchange session management and control information between connected devices. Unlike S-frames, U-frames contain an information field, but one used for system management information, not user data. As with S-frames, however, much of the information carried by U-frames is contained in codes included in the control field. U-frame codes are divided into two sections: a 2-bit prefix before the PtF bit and a 3-bit suffix after the PtF bit. Together, these two segments (5 bits) can be used to create up to 32 different types of U-frames.

Q.2 b)

The neat diagram of OSI model.

LAYER 1: THE PHYSICAL LAYER

The bottom layer of the OSI Model is the Physical Layer. It addresses the physical characteristics of the network, such as the types of cables used to connect devices, the types of connectors used, how long the cables can be, and so on. For example, the Ethernet standard for 100BaseT cable specifies the electrical characteristics of the twisted-pair cables, the size and shape of the connectors, the maximum length of the cables, and so on. Another aspect of the Physical Layer is that it specifies the electrical characteristics of the signals used to transmit data over cables from one network node to another. The Physical Layer doesn’t define any particular meaning for those signals other than the basic binary values 0 and 1. The higher levels of the OSI model must assign meanings to the bits transmitted at the Physical Layer.

One type of Physical Layer device commonly used in networks is a repeater. A repeater is used to regenerate signals when you need to exceed the cable length allowed by the Physical Layer standard or when you need to redistribute a signal from one cable onto two or more cables.

An old-style 10BaseT hub is also a Physical Layer device. Technically, a hub is a multi-port repeater because its purpose is to regenerate every signal received on any port on all the hub's other ports. Repeaters and hubs don't examine the contents of the signals that they regenerate. If they did, they'd be working at the Data Link Layer, not at the Physical Layer.

LAYER 2: THE DATA LINK LAYER

The Data Link Layer is the lowest layer at which meaning is assigned to the bits that are transmitted over the network. Data-link protocols address things, such as the size of each packet of data to be sent, a means of addressing each packet so that it's delivered to the intended recipient, and a way to ensure that two or more nodes don't try to transmit data on the network at the same time.

The Data Link Layer also provides basic error detection and correction to ensure that the data sent is the same as the data received. If an uncorrectable error occurs, the data-link standard must specify how the node is to be informed of the error so it can retransmit the data. At the Data Link Layer, each device on the network has an address known as the Media Access Control address, or MAC address. This is the actual hardware address, assigned to the device at the factory. You can see the MAC address for a computer's network adapter by opening a command window and running the ipconfig /all command.

LAYER 3: THE NETWORK LAYER

The Network Layer handles the task of routing network messages from one computer to another. The two most popular Layer-3 protocols are IP (which is usually paired with TCP) and IPX (normally paired with SPX for use with Novell and Windows networks). Logical addresses are created and used by Network Layer protocols, such as IP or IPX. The Network Layer protocol translates logical addresses to MAC addresses. For example, if you use IP as the Network Layer protocol, devices on the network are assigned IP addresses, such as 207.120.67.30. Because the IP protocol must use a Data Link Layer protocol to actually send packets to devices, IP must know how to translate the IP address of a device into the correct MAC address for the device. You can use the ipconfig command to see the IP address of your computer. Another important function of the Network layer is routing — finding an appropriate path through the network. Routing comes into play when a computer on one network needs to send a packet to a computer on another network. In this case, a Network Layer device called a router forwards the packet to the destination network. An important feature of routers is that they can be used to connect networks that use different Layer-2 protocols. For example, a router can be used to connect a local-area network that uses Ethernet to a wide-area network that runs on a different set of low-level protocols, such as T1.

LAYER 4: THE TRANSPORT LAYER

The Transport Layer is the basic layer at which one network computer communicates with another network computer. The Transport Layer is where you'll find one of the most popular networking protocols: TCP. The main purpose of the Transport Layer is to ensure that packets move over the network reliably and without errors. The Transport Layer does this by establishing connections between network devices, acknowledging the receipt of packets, and resending packets that aren't received or are corrupted when they arrive. In many cases, the Transport Layer protocol divides large messages into smaller packets that can be sent over the network efficiently. The Transport Layer protocol reassembles the message on the receiving end, making sure that all packets contained in a single transmission are received and no data is lost.

LAYER 5: THE SESSION LAYER

The Session Layer establishes sessions (instances of communication and data exchange) between network nodes. A session must be established before data can be transmitted over the network. The Session Layer makes sure that these sessions are properly established and maintained.

LAYER 6: THE PRESENTATION LAYER

The Presentation Layer is responsible for converting the data sent over the network from one type of representation to another. For example, the Presentation Layer can apply sophisticated compression techniques so fewer bytes of data are required to represent the information when it's sent over the network. At the other end of the transmission, the Transport Layer then uncompresses the data. The Presentation Layer also can scramble the data before it's transmitted and then unscramble it at the other end, using a sophisticated encryption technique.

LAYER 7: THE APPLICATION LAYER

The highest layer of the OSI model, the Application Layer, deals with the techniques that application programs use to communicate with the network. The name of this layer is a little confusing because application programs (such as Excel or Word) aren't actually part of the layer. Rather, the Application Layer represents the level at which application programs interact with the network, using programming interfaces to request network services. One of the most commonly used application layer protocols is HTTP, which stands for HyperText Transfer Protocol. HTTP is the basis of the World Wide Web.

Q.3 a)

A **distance-vector routing (DVR)** protocol requires that a router inform its neighbors of topology changes periodically. Historically known as the old ARPANET routing algorithm (or known as Bellman-Ford algorithm).

Bellman Ford Basics – Each router maintains a Distance Vector table containing the distance between itself and ALL possible destination nodes. Distances,based on a chosen metric, are computed using information from the neighbors' distance vectors.

```
Information kept by DV router -
```

- Each router has an ID
- Associated with each link connected to a router,
- there is a link cost (static or dynamic).
- Intermediate hops

```
Distance Vector Table Initialization -
```

- Distance to itself = 0
- Distance to ALL other routers = infinity number.

Distance Vector Algorithm –

1. A router transmits its distance vector to each of its neighbors in a routing packet.
2. Each router receives and saves the most recently received distance vector from each of its neighbors.
3. A router recalculates its distance vector when:
   - It receives a distance vector from a neighbor containing different information than before.
   - It discovers that a link to a neighbor has gone down.

The DV calculation is based on minimizing the cost to each destination

```
Dx(y) = Estimate of least cost from x to y

C(x,v) =  Node x knows cost to each neighbor v

Dx   =  [Dx(y): y ∈ N ] = Node x maintains distance vector

Node x also maintains its neighbors' distance vectors

– For each neighbor v, x maintains Dv = [Dv(y): y ∈ N ]
```

Note –

- From time-to-time, each node sends its own distance vector estimate to neighbors.
- When a node x receives new DV estimate from any neighbor v, it saves v's distance vector and it updates its own DV using B-F equation:

```
Dx(y) = min { C(x,v) + Dv(y)} for each node y ∈ N
```

Note:- give one example of DVR.

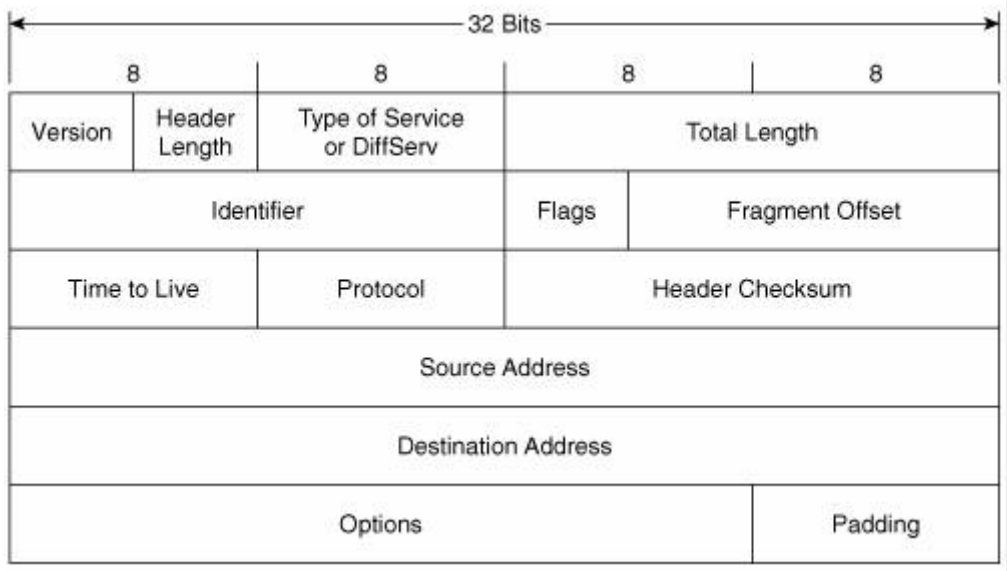
Q.3 b)

-Give at least 5 points difference between stop and wait and sliding window protocols with suitable example.

- explain selective repeat ARQ with suitable example.

Q.4 a)

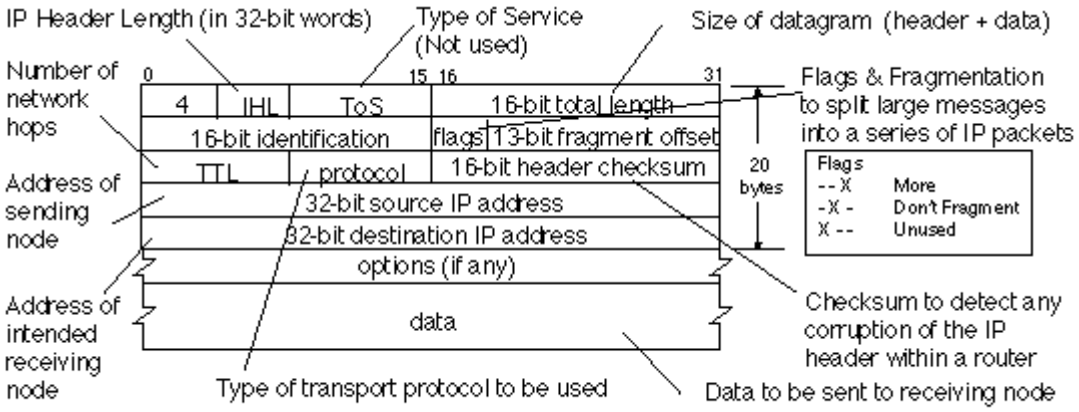
Internet Protocol version 4 (**IPv4**) is the fourth revision in the development of the Internet Protocol (IP) and the first version of the protocol to be widely deployed. Together with IPv6, it is at the core of standards-based internetworking methods of the Internet
IPv4 is a connectionless protocol for use on packet-switched Link Layer networks (e.g., Ethernet). It operates on a best effort delivery model, in that it does not guarantee delivery, nor does it assure proper sequencing or avoidance of duplicate delivery. These aspects, including data integrity, are addressed by an upper layer transport protocol , such as the Transmission Control Protocol (TCP).



IPv4 Header

The IPv4 packet header consists of 14 fields, of which 13 are required. The 14th field is optional named: options. The IPv4 packet header consists of 20 bytes of data.

- **Version**:- The first header field in an IP packet is the four-bit version field. The Version field indicates the format of the internet header. Version identifies the IP version to which the packet belongs. This four-bit field is set to binary 0100 to indicate version 4 (IPv4) or binary 0110 to indicate version 6 (IPv6).



- **Header length or Internet Header Length (IHL) :-** The second field (4 bits) is the Internet Header Length (IHL) telling the number of 32-bit words in the header. Since an IPv4 header may contain a variable number of options, this field specifies the size of the header (this also coincides with the offset to the data). The minimum value for this field is 5 , which is a length of 5×32 = 160 bits = 20 bytes. Being a 4-bit value, the maximum length is 15 words (15×32 bits) or 480 bits = 60 bytes.
- **Type of Service(ToS):–** now known as **Differentiated Services Code Point (DSCP).** The TOS field is used to carry information to provide quality of service features. New technologies are emerging that require real-time data streaming and therefore make use of the DSCP field. An example is Voice over IP (VoIP) that is used for interactive data voice exchange.

TOS allows the selection of a delivery service in terms of precedence, throughput, delay, reliability, and monetary cost.

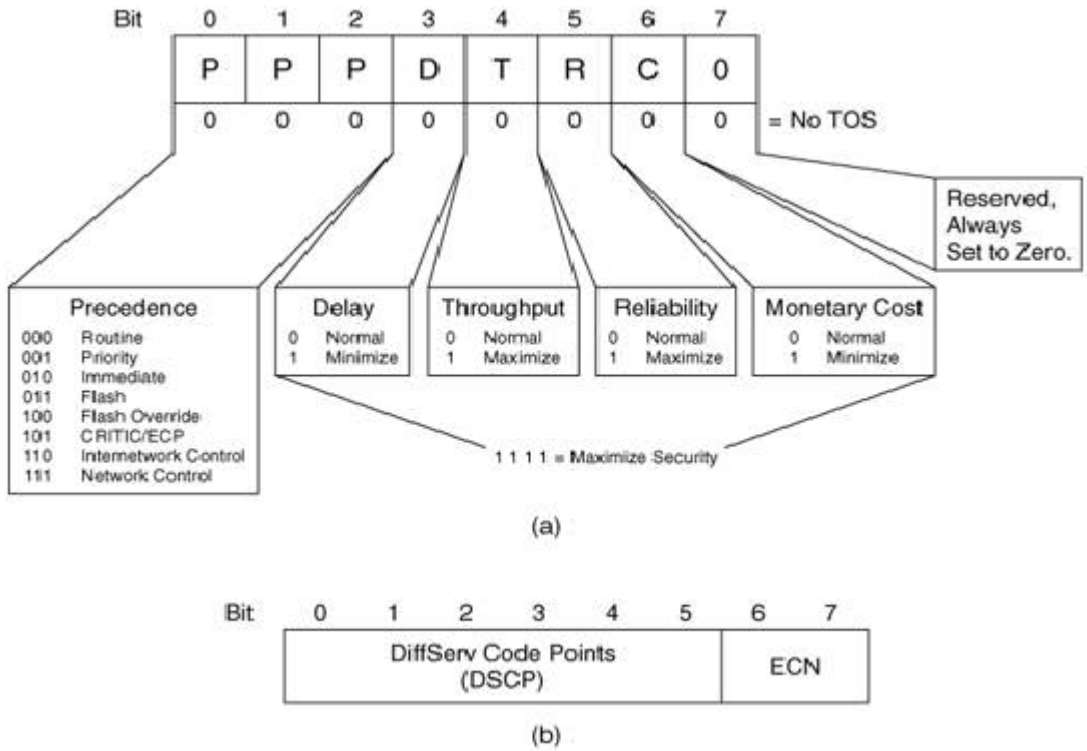
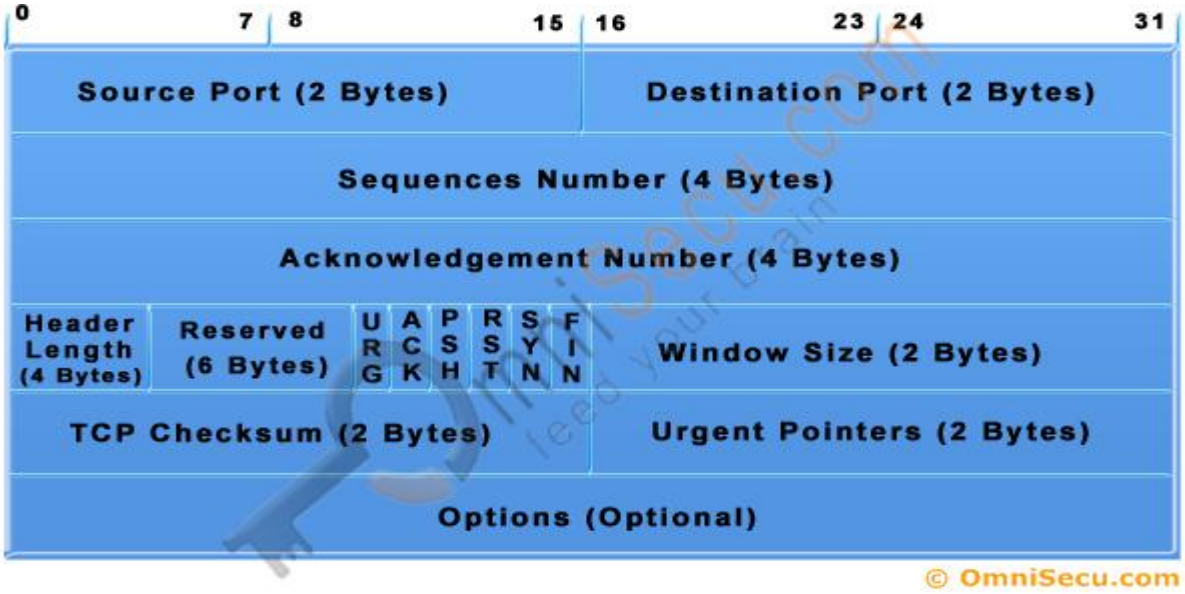


Fig:-(a) Type of Service and (b) DSCP & ECN

- **Explicit Congestion Notification (ECN) :-It** allows end-to-end notification of network congestion without dropping packets. ECN is an optional feature that is only used when both endpoints support it and are willing to use it. It is only effective when supported by the underlying network.
- **Total Length:-** This 16-bit field defines the entire datagram size, including header and data, in bytes. The minimum-length datagram is 20 bytes (20-byte header + 0 bytes data) and the maximum is 65,535 bytes — the maximum value of a 16-bit word. The minimum size datagram that any host is required to be able to handle is 576 bytes, but most modern hosts handle much larger packets. Sometimes subnetworks impose further restrictions on the size, in which case datagrams must be fragmented. Fragmentation is handled in either the host or packet switch in IPv4.
- **Identification:–** This field is an identification field and is primarily used for uniquely identifying fragments of an original IP datagram. Some experimental work has suggested using the ID field for other purposes, such as for adding packet-tracing information to datagrams in order to help trace back datagrams with spoofed source addresses.
- **Flags:–**A three-bit field follows and is used to control or identify fragments. They are (in order, from high order to low order):
  - bit 0: Reserved; must be zero.
  - bit 1: Don't Fragment (DF)
  - bit 2: More Fragments (MF)
- **Don't Fragment:-** Sets the Don't Fragment bit in sent packets. When an IP datagram has its DF flag set, intermediate devices are not allowed to fragment it so if it needs to travel across a network with a MTU(Maximum Transmission Unit) smaller that datagram length the datagram will have to be dropped. Normally an ICMP Destination Unreachable message is generated and sent back to the sender.
- **More Fragments:-** Sets the More Fragments bit in sent packets. The MF flag is set to indicate the receiver that the current datagram is a fragment of some larger datagram. When set to zero it indicates that the current datagram is either the last fragment in the set or that it is the only fragment.
- **Fragment Offset:-**The fragment offset field, measured in units of eight-byte blocks, is 13 bits long and specifies the offset of a particular fragment relative to the beginning of the original unfragmented IP datagram. The first fragment has an offset of zero. This allows a maximum offset of $(2^{13} – 1) \times 8 = 65{,}528$ bytes which would exceed the maximum IP packet length of 65,535 bytes with the header length included (65,528 + 20 = 65,548 bytes).
- **Time To Live (TTL):-**It is of 8 bit field. This field indicates the maximum time the datagram is allowed to remain in the internet system. If this field contains the value zero, then the datagram must be destroyed. This field is modified in internet header processing. The time is measured in units of seconds, but since every module that processes a datagram must decrease the TTL by at least one even if it process the datagram in less than a second, the TTL must be thought of only as an upper bound on the time a datagram may exist. The intention is to cause undeliverable datagrams to be discarded, and to bound the maximum datagram lifetime. `<hops>` must be a number in the range [0–255].
- **Protocol:-**This field defines the protocol used in the data portion of the IP datagram. The Internet Assigned Numbers Authority maintains a list of IP protocol numbers.
- **Header Checksum:-** The 16-bit checksum field is used for error-checking of the header. At each hop, the checksum of the header must be compared to the value of this field. If a header checksum is found to be mismatched, then the packet is discarded. Errors in the data field must be handled by the encapsulated protocol and both UDP and TCP have checksum fields.

Q 5 a) In Transmission Control Protocol (TCP) Segment Header lesson, you will learn more about TCP Segment Header, different fields in TCP Header and the use of these fields.



Transmission Control Protocol (TCP) Segment Header.

Source port: 16 Bit number which identifies the Source Port number (Sending Computer's TCP Port).

Destination port: 16 Bit number which identifies the Destination Port number (Receiving Port).

Sequence number: 32 Bit number used for byte level numbering of TCP segments. If you are using TCP, each byte of data is assigned a sequence number. If SYN flag is set (during the initial three way handshake connection initiation), then this is the initial sequence number. The sequence number of the actual first data byte will then be this sequence number plus 1. For example, let the first byte of data by a device in a particular TCP header will have its sequence number in this field 50000. If this packet has 500 bytes of data in it, then the next packet sent by this device will have the sequence number of 50000 + 500 + 1 = 50501.

Acknowledgment Number: 32 Bit number field which indicates the next sequence number that the sending device is expecting from the other device.

Header Length: 4 Bit field which shows the number of 32 Bit words in the header. Also known as the Data Offset field. The minimum size header is 5 words (binary pattern is 0101).

Reserved: Always set to 0 (Size 6 bits).

Control Bit Flags: We have seen before that TCP is a Connection Oriented Protocol. The meaning of Connection Oriented Protocol is that, before any data can be transmitted, a reliable connection must be obtained and acknowledged. Control Bits govern the entire process of connection establishment, data transmissions and connection termination. The control bits are listed as follows: They are:

URG: Urgent Pointer.

ACK: Acknowledgement.

PSH: This flag means Push function. Using this flag, TCP allows a sending application to specify that the data must be pushed immediately. When an application requests the TCP to push data, the TCP should send the data that has accumulated without waiting to fill the segment.

RST: Reset the connection. The RST bit is used to RESET the TCP connection due to unrecoverable errors. When an RST is received in a TCP segment, the receiver must respond by immediately terminating the connection. A RESET causes both sides immediately to release the connection and all its resources. As a result, transfer of data ceases in both directions, which can result in loss of data that is in transit. A TCP RST indicates an abnormal terminination of the connection.

SYN: This flag means synchronize sequence numbers. Source is beginning a new counting sequence. In other words, the TCP segment contains the sequence number of the first sent byte (ISN).

FIN: No more data from the sender. Receiving a TCP segment with the FIN flag does not mean that transferring data in the opposite direction is not possible. Because TCP is a fully duplex connection, the FIN flag will cause the closing of connection only in one direction. To close a TCP connection gracefully, applications use the FIN flag.

Window: indicates the size of the receive window, which specifies the number of bytes beyond the sequence number in the acknowledgment field that the receiver is currently willing to receive.

Checksum: The 16-bit checksum field is used for error-checking of the header and data.

Urgent Pointer: Shows the end of the urgent data so that interrupted data streams can continue. When the URG bit is set, the data is given priority over other data streams (Size 16 bits).

In this lesson, you have learned different fields in Transmission Control Protocol (TCP) Segment Header and the use of these fields. The fields in Transmission Control Protocol (TCP) Segment Header are Source Port, Destination Port, Sequence Number, Acknowledgement Number, Header Length, Flags, Window Size,

TCP Checksum and Urgent Pointer. Click "Next" to continue.

Q. 5 b) Definition of routing..

Explanation, algorithm of OSPF/

Example of OSPF.

Q 6. a)

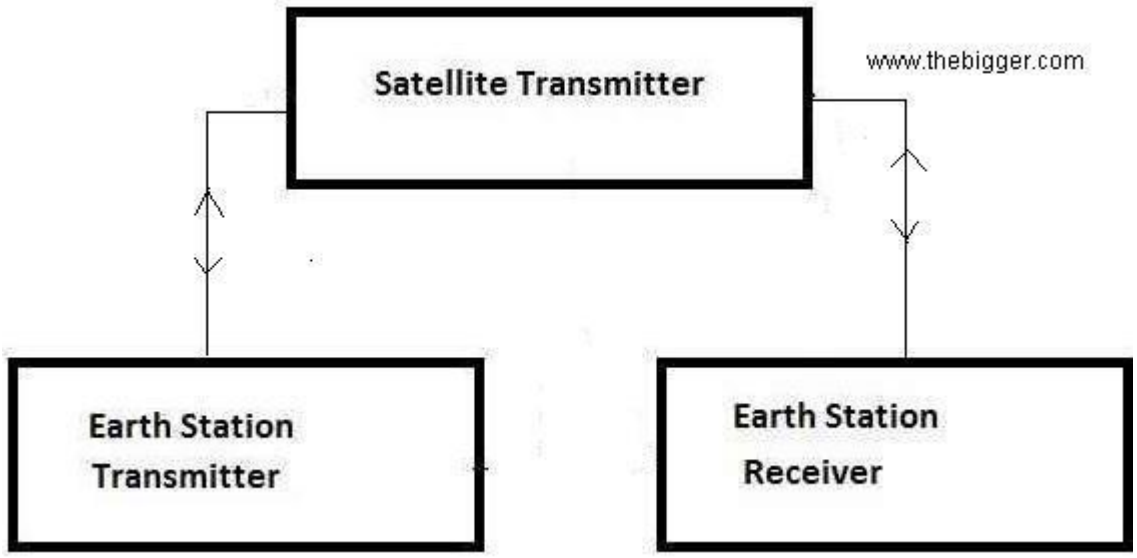
What is Satellite Communication?

In satellite communication, signal transferring between the sender and receiver is done with the help of satellite. In this process, the signal which is basically a beam of modulated microwaves is sent towards the satellite. Then the satellite amplifies the signal and sent it back to the receiver's antenna present on the earth's surface. So, all the signal transferring is happening in space. Thus this type of communication is known as space communication.

Two satellites which are commonly used in satellite communication are Active and passive satellites.

Passive satellites: It is just a plastic balloon having a metal coated over it. This sphere reflects the coming microwave signals coming from one part of the earth to other part. This is also known as passive sphere. Our earth also has a passive satellite i.e. moon.

Active satellites: It basically does the work of amplifying the microwave signals coming. In active satellites an antenna system, transmitter, power supply and a receiver is used. These satellites are also called as transponders. The transmitters fitted on the earth generate the microwaves. These rays are received by the transponders attached to the satellite. Then after amplifying, these signals are transmitted back to earth. This sending can be done at the same time or after some delay. These amplified signals are stored in the memory of the satellites, when earth properly faces the satellite. Then the satellite starts sending the signals to earth. Some active satellites also have programming and recording features. Then these recording can be easily played and watched. The first active satellite was launched by Russia in 1957. The signals coming from the satellite when reach the earth, are of very low intensity. Their amplification is done by the receivers themselves. After amplification these become available for further use.

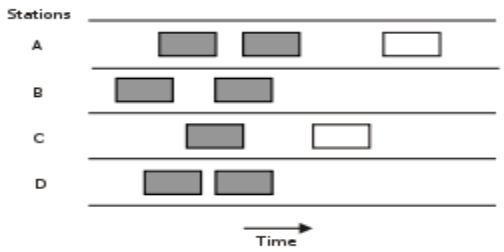


b)

ALOHA : ALOHAnet, also known as the ALOHA System, or simply ALOHA, was a pioneering computer networking system.The ALOHAnet used a new method of medium access (ALOHA random access) and experimental ultra high frequency (UHF) for its operation.

There are two types of ALOHA :

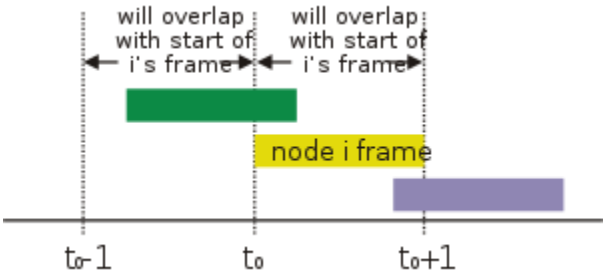
1. Pure ALOHA :



Pure ALOHA protocol. Boxes indicate frames. :

- If you have data to send, send the data
- If, while you are transmitting data, you receive any data from another station, there has been a message collision. All transmitting stations will need to try resending "later".

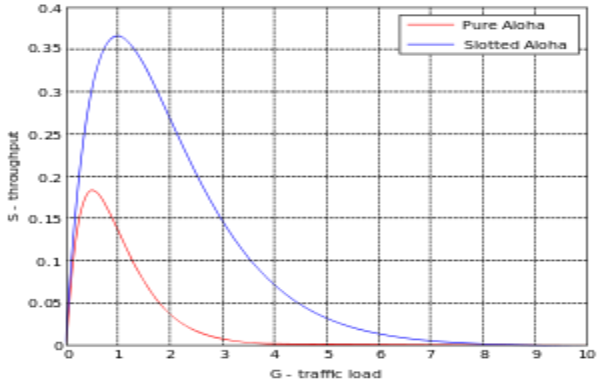
Let "*T*" that is, on average, there are *G* transmission-attempts per frame-time.



Overlapping frames in the pure ALOHA protocol. Frame-time is equal to 1 for all frames.

For any frame-time, the probability of there being *k* transmission-attempts during that frame-time is:

$$\frac{G^k e^{-G}}{k!}$$



Comparison of Pure Aloha and Slotted Aloha shown on Throughput vs. Traffic Load plot.

The average amount of transmission-attempts for 2 consecutive frame-times is 2*G*. two frame-times is:

$$\frac{(2G)^k e^{-2G}}{k!}$$

Therefore, the probability ($Prob_{pure}$) of there being zero transmission-attempts between *t*-*T* and *t*+*T*(and thus of a successful transmission for us) is:

$$Prob_{pure} = e^{-2G}$$

it can be concluded that the throughput (S_{pure}) is:

$$S_{pure} = Ge^{-2G}$$ Vulnerable time=2*T.

then by using Poisson distribution, the probability that exactly x nodes begin transmission during period T is

$$P[X = x] = \frac{G^x e^{-G}}{x!}$$

Therefore, the probability that during any particular period from t=2nT to t=(2n+1)T, exactly one node will begin transmission is

$$P[X = 1] = \frac{G^1 e^{-G}}{1!} = Ge^{-G}$$

And the probability that during any particular period t=(2n+1)T to t=(2n+2)T, no node will begin transmission is

$$P[X = 0] = \frac{G^0 e^{-G}}{0!} = e^{-G}$$

That is during period t=2nT to t=(2n+1)T, exactly one node begins transmission and during t=(2n+1)T to t=(2n+2)T no node begins transmission

$$P = P(0) \times P(1) = Ge^{-G} \times e^{-G} = Ge^{-2G}$$

This is the throughput. Therefore, the throughput in pure ALOHA,

$$S_{pure} = Ge^{-2G}$$

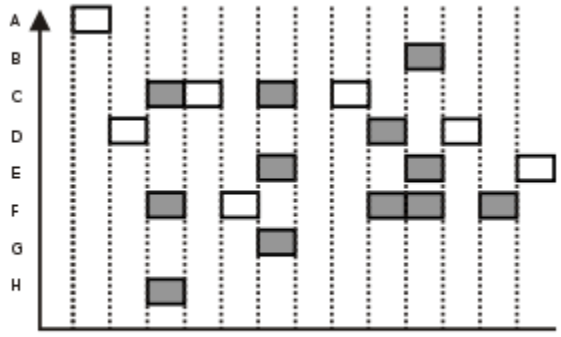
Similarly for slotted ALOHA, a frame will be successfully transmitted.

$$P[X = 1] = \frac{G^1 e^{-G}}{1!} = Ge^{-G}$$

This is the throughput in slotted ALOHA. Thus,

$$S_{slotted} = Ge^{-G}$$

2. Slotted ALOHA :



Slotted ALOHA protocol (shaded slots indicate collision)

Slotted ALOHA protocol.

An improvement to the original ALOHA protocol was "Slotted ALOHA".

$$Prob_{slotted} = e^{-G}$$

the probability of k packets is:

$$Prob_{slotted}k = e^{-G}(1 - e^{-G})^{k-1}$$

The throughput is:

$$S_{slotted} = Ge^{-G}$$

The maximum throughput is *1/e* frames per frame-time (reached when *G* = 1), which is approximately 0.368 frames per frame-time, or 36.8%.

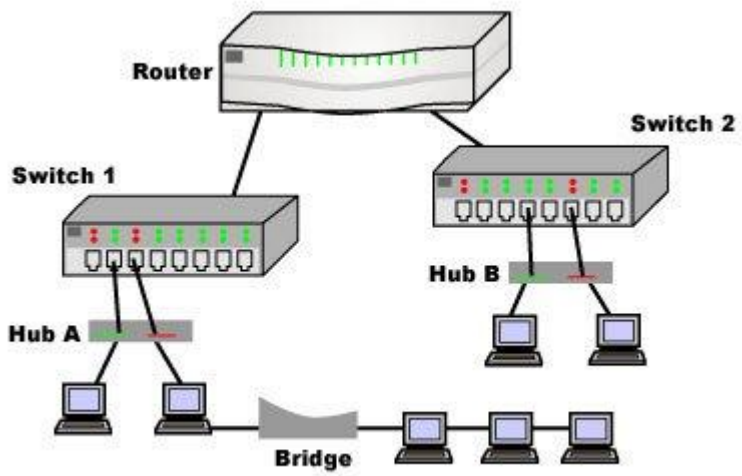
c)

Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do no amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

Switch – A switch is a multi port bridge with a buffer and a design that can boost its efficiency(large number of ports imply less traffic) and performance. Switch is data link layer device. Switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets

selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains same

Gateway – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.



d)

TCP implementation uses four timers –

1. **Retransmission Timer –** To retransmit lost segments, TCP uses retransmission timeout (RTO). When TCP sends a segment the timer starts and stops when the acknowledgment is received. If the timer expires timeout occurs and the segment is retransmitted. RTO (retransmission timeout is for 1 RTT) to calculate retransmission timeout we first need to calculate the RTT(round trip time).

RTT three types –

- **Measured RTT(RTTm) –** The measured round-trip time for a segment is the time required for the segment to reach the destination and be acknowledged, although the acknowledgment may include other segments.
- **Smoothed RTT(RTTs) –** It is the weighted average of RTTm. RTTm is likely to change and its fluctuation is so high that a single measurement cannot be used to calculate RTO.

```
▪ Initially -> No value
▪ After the first measurement -> RTTs=RTTm
▪ After each measurement -> RTTs= (1-t)*RTTs + t*RTTm
▪ Note: t=1/8 (default if not given)
```

- **Deviated RTT(RTTd) –** Most implementation do not use RTTs alone so RTT deviated is also calculated to find out RTO.

```
Initially -> No value
After the first measurement -> RTTd=RTTm/2
After each measurement -> RTTd= (1-k)*RTTd + k*(RTTm-RTTs)
Note: k=1/4 (default if not given)
```

Retransmission Timeout : RTO calculation – The value of RTO is based on the smoothed round-trip time and its deviation. Most implementations use the following formula to calculate the RTO:

```
Initial value -> Original (given in question)
After any measurement -> RTO=RTTs + 4*RTTd
```

#NOTE: At every retransmission the value of RTO doubles. (RTO(new) = RTO(before retransmission) *2) this is explained in Karn's Algorithm

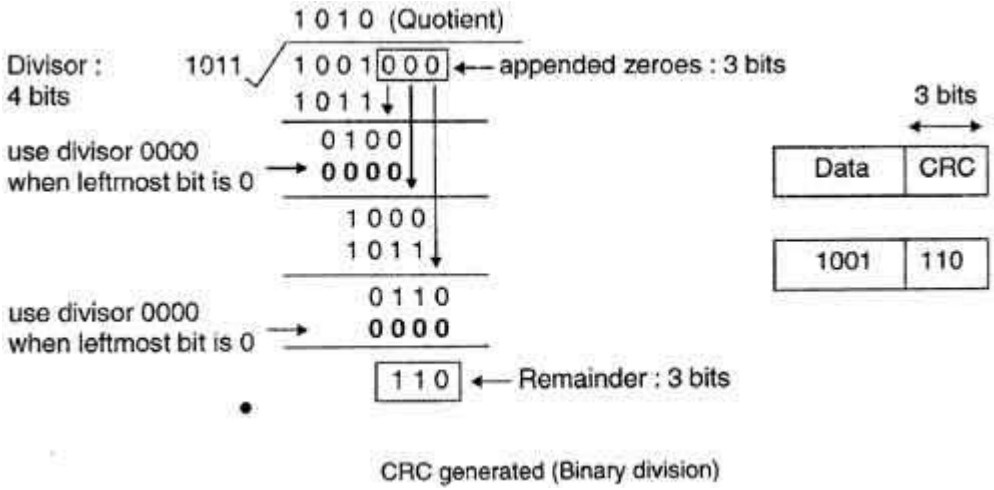
2. **Persistent Timer –** To deal with a zero-window-size deadlock situation, TCP uses a persistence timer.When the sending TCP receives an acknowledgment with a window size of zero, it starts a persistence timer. When the persistence timer goes off, the sending TCP sends a special segment called a probe. This segment contains only 1 byte of new data. It has a sequence number, but its sequence number is never acknowledged; it is even ignored in calculating the sequence number for the rest of the data. The probe causes the receiving TCP to resend the acknowledgment which was lost.
3. **Keep Alive Timer –** A keepalive timer is used to prevent a long idle connection between two TCPs. If a client opens a TCP connection to a server transfers some data and becomes silent the client will crash. In this case, the connection remains open forever. So a keepalive timer is used. Each time the server hears from a client, it resets this timer. The time-out is usually 2 hours. If the server does not hear from the client after 2 hours, it sends a probe segment.If there is no response after 10 probes, each of which is 75 s apart, it assumes that the client is down and terminates the connection.
4. **Time Wait Timer –** This timer is used during tcp connection termination. The timer starts after sending the last Ack for 2nd FIN and closing the connection.

e)

Cyclic Redundancy Check (CRe) An error detection mechanism in which a special number is appended to a block of data in order to detect any changes introduced during storage (or transmission). The CRe is recalculated on retrieval (or reception) and compared to the value originally transmitted, which can reveal certain types of error. For example, a single corrupted bit in the data results in a one-bit change in the calculated CRC, but multiple corrupt bits may cancel each other out.A CRC is derived using a more complex algorithm than the simple CHECKSUM, involving MODULO ARITHMETIC (hence the 'cyclic' name) and treating each input word as a set of coefficients for a polynomial. CRC is more powerful than VRC and LRC in detecting errors. It is not based on binary addition like VRC and LRC. Rather it is based on binary division. At the sender side, the data unit to be transmitted IS divided by a predetermined divisor (binary number) in order to obtain the remainder. This remainder is called CRC.• The CRC has one bit less than the divisor. It means that if CRC is of n bits, divisor is of n+ 1 bit.• The sender appends this CRC

to the end of data unit such that the resulting data unit becomes exactly divisible by predetermined divisor i.e. remainder becomes zero.• At the destination, the incoming data unit i.e. data + CRC is divided by the same number (predetermined binary divisor).• If the remainder after division is zero then there is no error in the data unit & receiver accepts it.• If remainder after division is not zero, it indicates that the data unit has been damaged in transit and therefore it is rejected.• This technique is more powerful than the parity check and checksum error detection.• CRC is based on binary division. A sequence of redundant bits called CRC or CRC remainder is appended at the end of a data unit such as byte

1. Data unit 1011000 is divided by 1011.



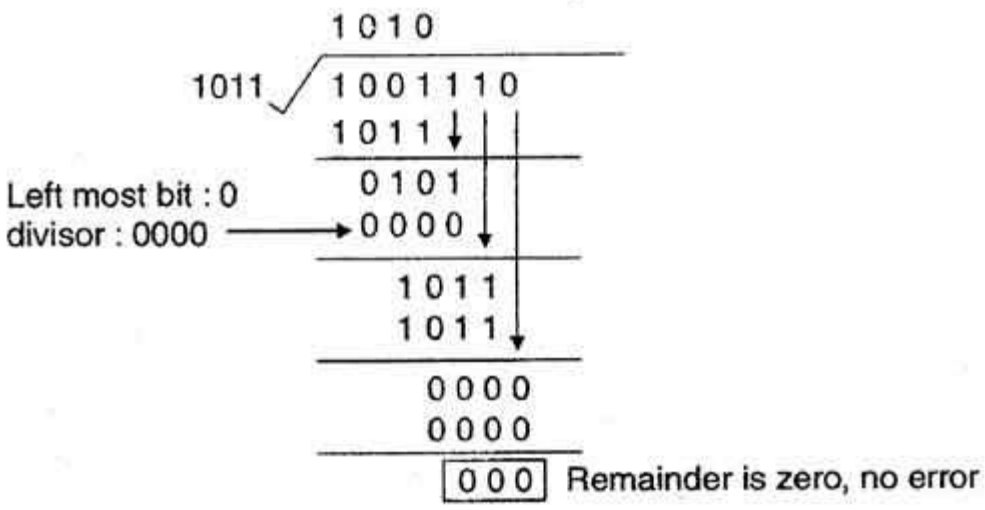
CRC generated (Binary division)

2. During this process of division, whenever the leftmost bit of dividend or remainder is 0, we use a string of Os of same length as divisor. Thus in this case divisor 1011 is replaced by 0000.

3. At the receiver side, data received is 1001110.

4. This data is again divided by a divisor 1011.

5. The remainder obtained is 000; it means there is no error.



CRC decoded (binary division)