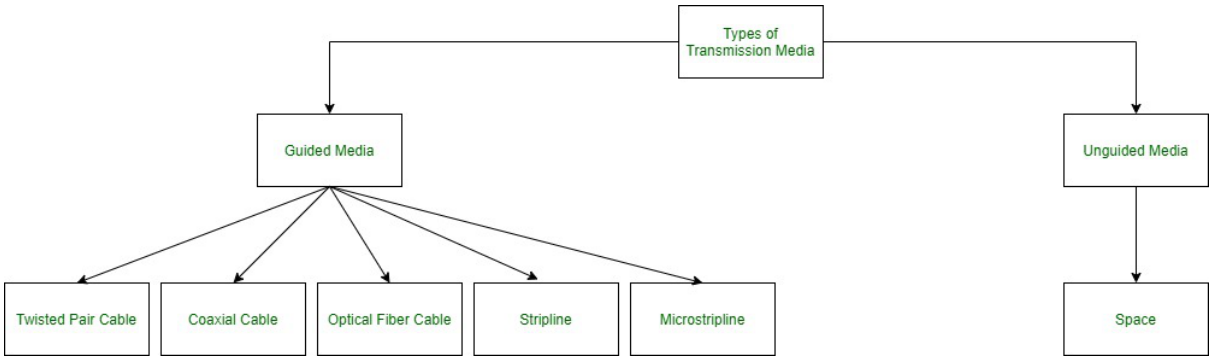
B. Tech.
(SEM-VI) THEORY EXAMINATION 2021-22
COMPUTER NETWORKS (KCS603)
Time: 3 Hours ***Total Marks: 100***

Note: Attempt all Sections. If you require any missing data, then choose suitably.

SECTION A

Q. 1 a: Discuss about transmission mediums in networking.

Solution: In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver i.e. it is the channel through which data is sent from one place to another. Transmission Media is broadly classified into the following types:



Q. 1 b: What do you understand by network topologies.

Solution: A Network Topology is the arrangement with which computer systems or network devices are connected to each other. Topologies may define both physical and logical aspect of the network. Both logical and physical topologies could be same or different in a same network.

Point-to-Point

Point-to-point networks contains exactly two hosts such as computer, switches or routers, servers connected back to back using a single piece of cable. Often, the receiving end of one host is connected to sending end of the other and vice-versa.

Bus Topology

In case of Bus topology, all devices share single communication line or cable. Bus topology may have problem while multiple hosts sending data at the same time. Therefore, Bus topology either uses CSMA/CD technology or recognizes one host as Bus Master to solve the issue.

Star Topology

All hosts in Star topology are connected to a central device, known as hub device, using a point-to-point connection. That is, there exists a point to point connection between hosts and hub.

Ring Topology

In ring topology, each host machine connects to exactly two other machines, creating a circular network structure. When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts.

Mesh Topology

In this type of topology, a host is connected to one or multiple hosts. This topology has hosts in point-to-point connection with every other host or may also have hosts which are in point-to-point connection to few hosts only.

Tree Topology

Also known as Hierarchical Topology, this is the most common form of network topology in use presently. This topology imitates as extended Star topology and inherits properties of bus topology.

Q. 1 c: Explain transmission delay in flow control.

Solution: The time taken to transmit a packet from the host to the transmission medium is called Transmission delay.

For example, if bandwidth is 1 bps (every second 1 bit can be transmitted onto the transmission medium) and data size is 20 bits then what is the transmission delay? If in one second, 1 bit can be transmitted. To transmit 20 bits, 20 seconds would be required.

Let B bps is the bandwidth and L bit is the size of the data then transmission delay Tt is,

$$Tt = L/B$$

Q. 1 d: Write a note on round trip time (RTT) in networking.

Solution: Round Trip Time (RTT) is the length time it takes for a data packet to be sent to a destination plus the time it takes for an acknowledgment of that packet to be received back at the origin. The RTT between a network and server can be determined by using the ping command.

Q. 1 e: Discuss the role logical addressing.

Solution: Logical Address is generated by CPU while a program is running. The logical address is virtual address as it does not exist physically, therefore, it is also known as Virtual Address. This address is used as a reference to access the physical memory location by CPU. The term Logical Address Space is used for the set of all logical addresses generated by a program's perspective.

The hardware device called Memory-Management Unit is used for mapping logical address to its corresponding physical address.

Mainly deals by IP addresses.

Q. 1 f: Define datagrams in switching.

Solution: The characteristics of the datagram packet switching are explained below −

1. In a datagram packet switched network the data packets follow their own path to send the packets between the source and destination.
2. During data transmission, after each packet reaches a node, then it decides which path the packet needs to follow the next.

3. This dynamic decision making of datagram packet switched networks improves the performance of data transmission.

Q. 1 g: Discuss about the IP ranges of Class A, B, C and D.

Solution:

Class A

00000001 – 01111111
1 – 127

Class B

10000000 – 10111111
128 – 191

Class C

11000000 – 11011111
192 – 223

Class D

11100000 – 11101111
224 – 239

Q. 1 h: List out prime three functionality of transport layer.

Solution: Prime functionality of transport layer are-

1. Process to process delivery
2. End-to-end Connection between hosts
3. Multiplexing and Demultiplexing
4. Congestion Control

Q. 1 i: Explain the use of RST flag in TCP header.

Solution: Reset (RST) – It is used to terminate the connection if the RST sender feels something is wrong with the TCP connection or that the conversation should not exist. It can get send from receiver side when packet is sent to particular host that was not expecting it.

Q. 1 j: Explain HTTP.

Solution: The Hypertext Transfer Protocol (HTTP) is the foundation of the World Wide Web, and is used to load web pages using hypertext links. HTTP is an application layer protocol designed to transfer information between networked devices and runs on top of other layers of the network protocol stack.

SECTION B

Q. 2 a: Discuss encoding types in physical layer of ISO-OSI model.

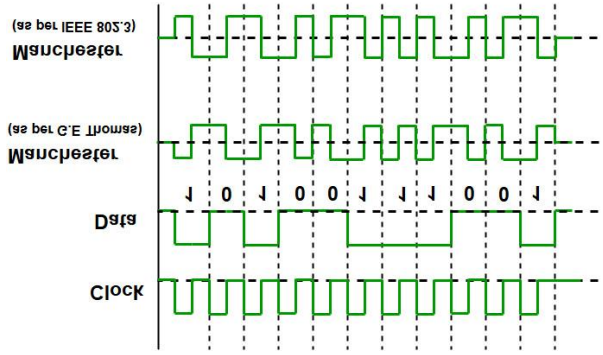
Solution: Here we mainly deals with Manchester encoding, It is a synchronous clock encoding technique used by the physical layer of the Open System Interconnection [OSI] to encode the clock and data of a synchronous bit stream. The idea of RZ and the idea of-L are combined in manchester

Different encoding techniques are used in data communication to ensure data security and transmission speed. Manchester encoding is an example of digital encoding. Because each data bit length is defined by default, it differs from other digital encoding schemes. The bit state is defined by the direction of the transition. Bit status is represented in various ways by different systems, although most systems use 1 bit for low to high transitions and 0 bit for high to low transitions.

In manchester duration of a bit is divided into two halves. The voltage remains the same at one level during the first half & moves to the other level. The transition at the middle of the bit provides synchronization. Differential Manchester,on the other hand, combines the idea of RZ and NRZ-I. There is always a transition at the middle of the bit, but the bit values are determined at the beginning of the bit. if next bit is zero there is transition if next bit is 1 there is none.

Note: Manchester encoding's main advantage is signal synchronization.

The binary data to be transmitted over the cable are not sent as NRZ [Non-return-to-zero].



Non-return-to-zero [NRZ] –

NRZ code's voltage level is constant during a bit interval. When there is a long sequence of 0s and 1s, there is a problem at the receiving end. The problem is that the synchronization is lost due to a lack of transmissions.

It is of 2 types:

(i) NRZ-level encoding –

The polarity of signals changes when the incoming signal changes from '1' to '0' or from '0' to '1'. It considers the first bit of data as polarity change.

(ii) NRZ-Inverted/ Differential encoding –

In this, the transitions at the beginning of the bit interval are equal to 1 and if there is no transition at the beginning of the bit interval is equal to 0.

Q. 2 b: Discuss each command in detail used in networking:

a- ipconfig
b- netstat
c- ping
d- hostname
e- tracert

Solution:

a- ipconfig: Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, ipconfig displays Internet Protocol version 4 (IPv4) and IPv6 addresses, subnet mask, and default gateway for all adapters.

b- netstat: Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). Used without parameters, this command displays active TCP connections.

c- ping: A ping (Packet Internet or Inter-Network Groper) is a basic Internet program that allows a user to test and verify if a particular destination IP address exists and can accept requests in computer network administration.

d- hostname: The hostname command is used to view or change a system's domain and hostname.

e- tracert: In computing, tracert are computer network diagnostic commands for displaying possible routes and measuring transit delays of packets across an Internet Protocol network.

Q. 2 c: List out and discuss the disadvantages in STOP N WAIT protocol.

Solution:

The following are the problems associated with a stop and wait protocol:

1. Problems occur due to lost data

Suppose the sender sends the data and the data is lost. The receiver is waiting for the data for a long time. Since the data is not received by the receiver, so it does not send any acknowledgment. Since the sender does not receive any acknowledgment so it will not send the next packet. This problem occurs due to the lost data.

In this case, two problems occur:

1. Sender waits for an infinite amount of time for an acknowledgment.
2. Receiver waits for an infinite amount of time for a data.

2. Problems occur due to lost acknowledgment

Suppose the sender sends the data and it has also been received by the receiver. On receiving the packet, the receiver sends the acknowledgment. In this case, the acknowledgment is lost in a network, so there is no chance for the sender to receive the acknowledgment. There is also no chance for the sender to send the next packet as in stop and wait protocol, the next packet cannot be sent until the acknowledgment of the previous packet is received.

In this case, one problem occurs:

1. Sender waits for an infinite amount of time for an acknowledgment.

3. Problem due to the delayed data or acknowledgment

Suppose the sender sends the data and it has also been received by the receiver. The receiver then sends the acknowledgment but the acknowledgment is received after the timeout period on the sender's side. As the acknowledgment is received late, so acknowledgment can be wrongly considered as the acknowledgment of some other data packet.

Q. 2 d: Calculate the total number of transmissions that are required to send 10 data packets through GBN-3 and every 5th packet is lost.

Solution:

Total packets: 1,2,3,4,5,6,7,8,9,10

Total transmission required if every 5^{th} packet is lost: 1,2,3,4,5,6,7,5,6,7,8,9,7,8,9,10,9,10 = **18 transmissions**

Q. 2 e: Discuss in detail about ICMP role in network layer.

Solution: Internet Control Message Protocol (ICMP) works in the network layer of the OSI model and the internet layer of the TCP/IP model. It is used to send control messages to network devices and hosts. Routers and other network devices monitor the operation of the network. When an error occurs, these devices send a message using ICMP. Messages that can be sent include "destination unreachable", "time exceeded", and "echo requests".

ICMP is a network layer protocol.

ICMP messages are not passed directly to the data link layer. The message is first encapsulated inside the IP datagram before going to the lower layer.

Types of ICMP messages

Information Messages − In this message, the sender sends a query to the host or router and expects an answer. For example, A host wants to know if a router is alive or not.

Error-reporting message − This message report problems that a router or a host (destination) may encounter when it processes an IP packet.

Query Message − It helps a router or a network manager to get specific information from a router or another host.

Source Quench − It requests to decrease the traffic rate of message sending from source to destination.

Time Exceeded − When fragments are lost in a network the fragments hold by the router will be dropped and then ICMP will take the source IP from the discarded packet and inform the source, that datagram is discarded due to the time to live field reaches zero, by sending time exceeded message.

Fragmentation Required − When a router is unable to forward a datagram because it exceeds the MTU of the next-hop network and the DF (Don't Fragment) bit is set, the router is required to return an ICMP Destination Unreachable message to the source of the datagram, with the Code indicating fragmentation is needed and DF (Don’t Fragment) set.

Destination Unreachable − This error message indicates that the destination host, network, or port number that is specified in the IP packet is unreachable. This may happen due to the destination host device is down, an intermediate router is unable to find a path to forward the packet, and a firewall is configured to block connections from the source of the packet.

Redirect Message − A redirect error message is used when a router needs to tell a sender that it should use a different path for a specific destination. It occurs when the router knows a shorter path to the destination.

SECTION C

Q. 3 a: Define the relationship between transmission delay and propagation delay, if the efficiency is at least 50% in STOP N WAIT protocol.

Solution: With Transmission delay as Tt and propagation delay as Tp,

According to problem, $Tt/(Tt+2*Tp) \geq ½$

Hence, $Tt \geq (2*Tp)$ is the answer.

Q. 3 b: Find out window size and minimum sequence number in sliding window protocol, if Transmission delay (Tt)= 1 ms, Propagation delay (Tp)= 24.5 ms. (ms= milliseconds).

Solution:

Window size,

$Ws= 1+ (2*Tp)/Tt$

$Ws= 1+ (2*24.5)/1$

Window Size, Ws= 50 is the answer.

Minimum bits required for sequence number

Minimum bits required for sequence number= Seal function ($\log_2 Ws$)= Seal function ($\log_2 50$)= Seal function (5.6)= **6 is the answer.**

Q. 4 a: Explain distance vector routing (DVR) with working example in detail.

Solution: 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).

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:

(i) It receives a distance vector from a neighbor containing different information than before.

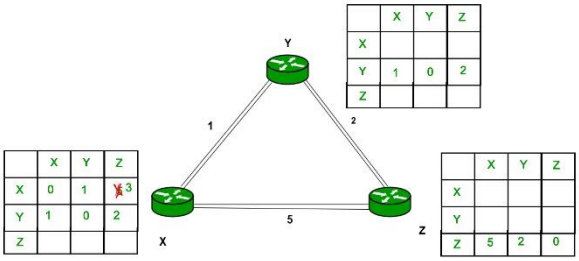
(ii) It discovers that a link to a neighbor has gone down.

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

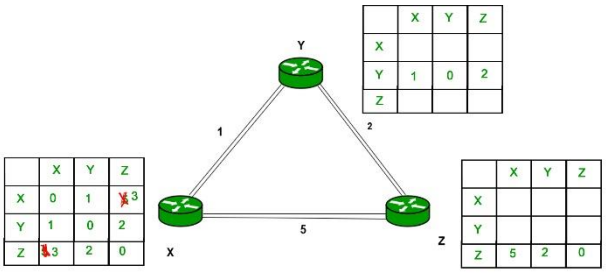
Example – Consider 3-routers X, Y and Z as shown in figure. Each router have their routing table. Every routing table will contain distance to the destination nodes.

Consider router X , X will share it routing table to neighbors and neighbors will share it routing table to it to X and distance from node X to destination will be calculated using bellmen- ford equation.

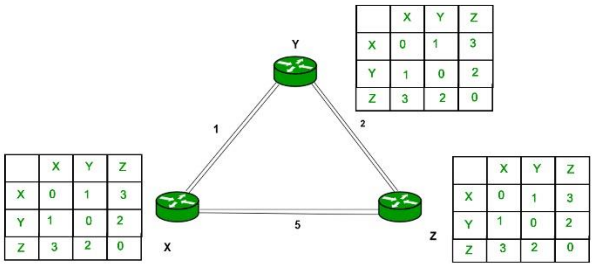
As we can see that distance will be less going from X to Z when Y is intermediate node(hop) so it will be update in routing table X.



Similarly for Z also –

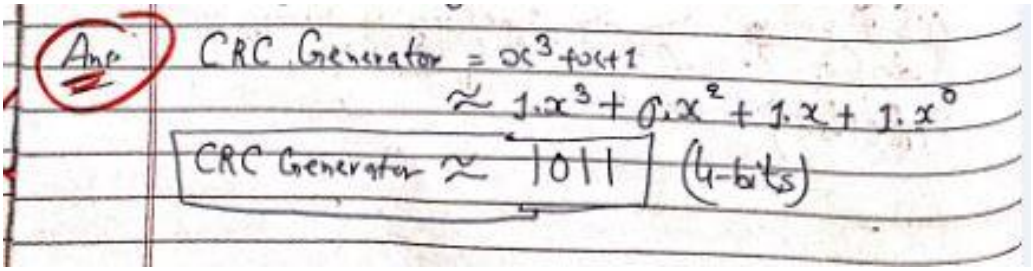


Finally the routing table for all –



Q. 4 b: Sender's data D=11010, CRC generator polynomial= x^3+x+1. Apply CRC algorithm and perform calculations both at sender and receiver end.

Solution:



Before starting the CRC algo. Both Sender & Receiver know about it. That is why CRC G. is available at both of them.

Now, as CRC G. is of 4-bits then take (n-1) 0's and apply (ex-OR) operation as we prev. discussed:-

11010 000
Actual data — 3 0's

⇒ 11010 000 → At Sender

(ex-OR) 1011

01100000
1011
01110 00
1011
00101 0
1011
0001 0 ⇒ STOR Here (No further space to apply CRC G.)

→ At Receiver

↳ CRC Code = 010

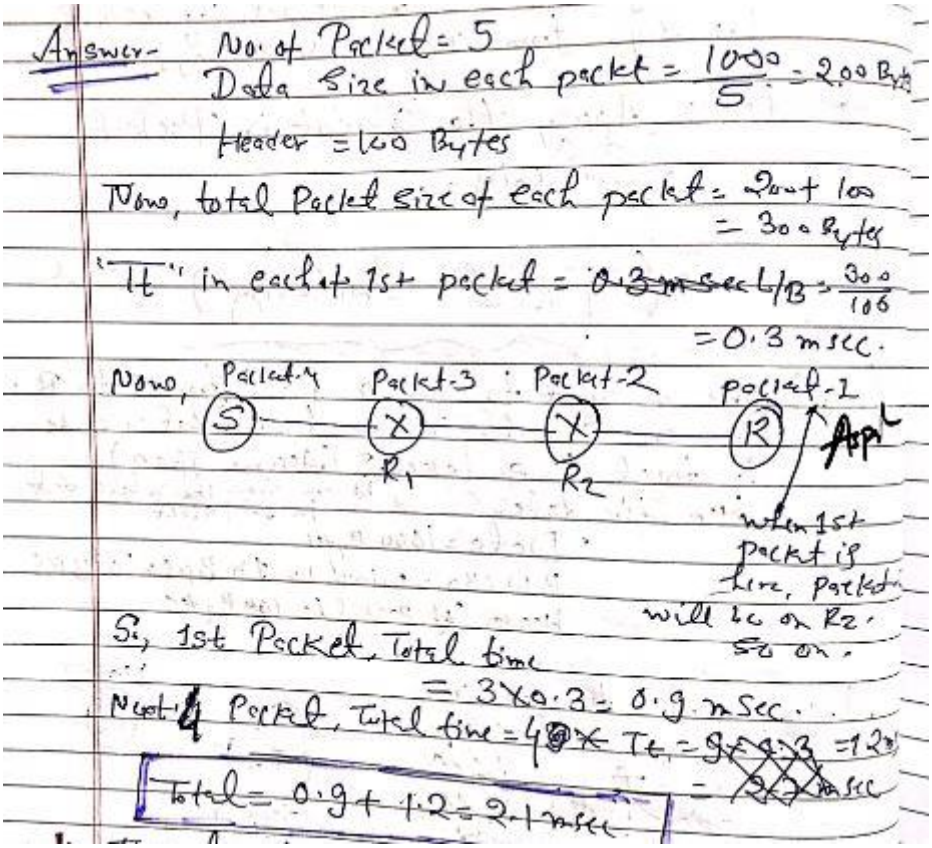
Again, 11010010
Actual data — CRC Code

⇒ 11010010
(ex-OR) 1011
01100010
1011
00111010
1011
00010110
1011
00000 0 ⇒ STOR here

As we have all 0's, so here NO Error.

Q. 5 a: Assume we want to send a data from S to R and there are 2 routers in between. What will be the total time taken if total number of packets are 5. Data is like:

Solution: 2.1 milliseconds



Q. 5 b: Explain CSMA/CD in detail.

Solution: CSMA/CD (Carrier Sense Multiple Access/ Collision Detection) is a media access control method that was widely used in Early Ethernet technology/LANs When there used to be shared

Bus Topology and each node (Computers) were connected By Coaxial Cables. Now a Days Ethernet is Full Duplex, and CSMA/CD is not used as Topology is either Star (connected via Switch or Router)

or Point to Point (Direct Connection) but they are still supported though.

How CSMA/CD works?

Step 1: Check if the sender is ready for transmitting data packets.

Step 2: Check if the transmission link is idle?

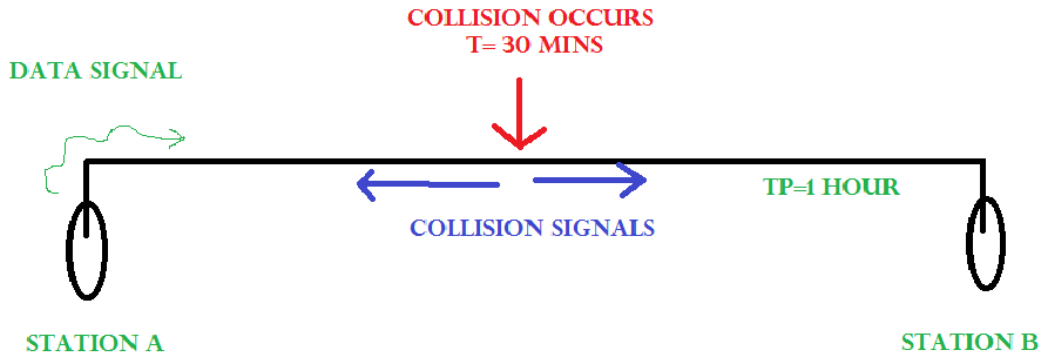
Sender has to keep on checking if the transmission link/medium is idle. For this, it continuously senses transmissions from other nodes. Sender sends dummy data on the link. If it does not receive any collision signal, this means the link is idle at the moment. If it senses that the carrier is free and there are no collisions, it sends the data. Otherwise, it refrains from sending data.

Step 3: Transmit the data & check for collisions.

Sender transmits its data on the link. CSMA/CD does not use an 'acknowledgment' system. It checks for successful and unsuccessful transmissions through collision signals. During transmission, if a collision signal is received by the node, transmission is stopped. The station then transmits a jam signal onto the link and waits for random time intervals before it resends the frame. After some random time, it again attempts to transfer the data and repeats the above process.

Step 4: If no collision was detected in propagation, the sender completes its frame transmission and resets the counters.

How does a station know if its data collide?



Consider the above situation. Two stations, A & B.

Propagation Time: Tp = 1 hr (Signal takes 1 hr to go from A to B)

At time t=0, A transmits its data.

t= 30 mins : Collision occurs.

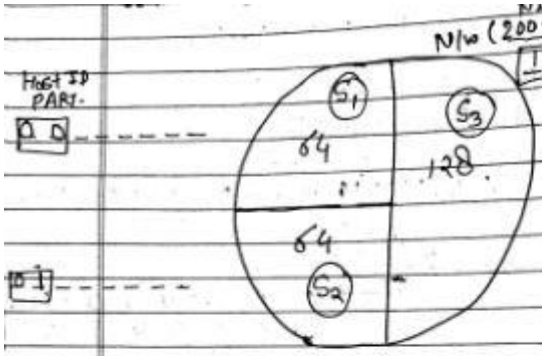
After the collision occurs, a collision signal is generated and sent to both A & B to inform the stations about a collision. Since the collision happened midway, the collision signal also takes 30 minutes to reach A & B.

Therefore, t=1 hr: A & B receive collision signals.

This collision signal is received by all the stations on that link.

Q. 6 a: Divide the network with IP address 200.1.2.0 into 5 subnets.

Solution: Here we have shown this network division into 3 variable subnets. Now any sub-network can further divided into 2 part to make it into 5-subnets. (All approaches are correct)



* 1st divide into 2-Parts. (by chosing 1-bit of HID)
* Then divide the 1st Subnet again into 2-parts again by chosing 1 more bit from HID.

In that Case.

S_1 ⇒ NID ⇒ 200.1.2.0
Subnet Mask ⇒ 255.255.255.192

S_2 ⇒ NID ⇒ 200.1.2.64
Subnet Mask ⇒ 255.255.255.192

S_3 ⇒ NID ⇒ 200.1.2.128
Subnet Mask ⇒ 255.255.255.128

So, For S_1 ⇒ 200.1.2.[0]

0 0 0 0 0 0 0 0 = 0
0 0 0 0 0 0 0 1 = 1
⋮
0 1 1 1 1 1 1 1 = 127

S_0 { NID = 200.1.2.0
DBA = 200.1.2.127 }

Subnet Mask ⇒ 11111111.11111111.11111111.10000000 ⇒ 255.255.255.128
(NID | SID | HID)

For S_2 ⇒ 200.1.2.[1 0]

0 0 0 0 0 0 = 128
0 0 0 0 0 1 = 129
⋮
1 1 1 1 1 1 = 191

S_0 { NID = 200.1.2.128
DBA = 200.1.2.191 }

Subnet Mask ⇒ 11111111.11111111.11111111.11000000 ⇒ 255.255.255.192
(NID | SID | HID)

For S_3 ⇒ 200.1.2.[1 1]

0 0 0 0 0 0 = 192
0 0 0 0 0 1 = 193
⋮
1 1 1 1 1 1 = 255

S_0 { NID = 200.1.2.192
DBA = 200.1.2.255 }

Subnet Mask ⇒ 11111111.11111111.11111111.11000000 ⇒ 255.255.255.192
(NID | SID | HID)

Q. 6 b: Describe the role of application layer and session layer of OSI model in detail.

Solution:

Application Layer

The Application Layer is topmost layer in the Open System Interconnection (OSI) model. This layer provides several ways for manipulating the data (information) which actually enables any type of user to access network with ease. This layer also makes a request to its bottom layer, which is presentation layer for receiving various types of information from it. The Application Layer interface directly interacts with application and provides common web application services. This layer is basically highest level of open system, which provides services directly for application process.

Functions of Application Layer :

1. Application Layer provides a facility by which users can forward several emails and it also provides a storage facility.
2. This layer allows users to access, retrieve and manage files in a remote computer.
3. It allows users to log on as a remote host.
4. This layer provides access to global information about various services.
5. This layer provides services which include: e-mail, transferring files, distributing results to the user, directory services, network resources and so on.
6. It provides protocols that allow software to send and receive information and present meaningful data to users.
7. It handles issues such as network transparency, resource allocation and so on.
8. This layer serves as a window for users and application processes to access network services.
9. Application Layer is basically not a function, but it performs application layer functions.
10. The application layer is actually an abstraction layer that specifies the shared protocols and interface methods used by hosts in a communication network.
11. Application Layer helps us to identify communication partners, and synchronizing communication.
12. This layer allows users to interact with other software applications.
13. In this layer, data is in visual form, which makes users truly understand data rather than remembering or visualize the data in the binary format (0’s or 1’s).
14. This application layer basically interacts with Operating System (OS) and thus further preserves the data in a suitable manner.
15. This layer also receives and preserves data from it’s previous layer, which is Presentation Layer (which carries in itself the syntax and semantics of the information transmitted).
16. The protocols which are used in this application layer depend upon what information users wish to send or receive.
17. This application layer, in general, performs host initialization followed by remote login to hosts.

Session Layer

The Session Layer is the 5th layer in the Open System Interconnection (OSI) model. This layer allows users on different machines to establish active communications sessions between them. It is responsible for establishing, maintaining, synchronizing, terminating sessions between end-user applications. In Session Layer, streams of data are received and further marked, which is then resynchronized properly, so that the ends of the messages are not cut initially and further data loss is avoided. This layer basically establishes a connection between the session entities. This layer handles and manipulates data which it receives from the Session Layer as well as from the Presentation Layer.

Functions of Session Layer :

1. Session Layer works as a dialog controller through which it allows systems to communicate in either half-duplex mode or full duplex mode of communication.
2. This layer is also responsible for token management, through which it prevents two users to simultaneously access or attempting the same critical operation.
3. This layer allows synchronization by allowing the process of adding checkpoints, which are considered as synchronization points to the streams of data.
4. This layer is also responsible for session checkpointing and recovery.
5. This layer basically provides a mechanism of opening, closing and managing a session between the end-user application processes.
6. The services offered by Session Layer are generally implemented in application environments using remote procedure calls (RPCs).
7. The Session Layer is also responsible for synchronizing information from different sources.
8. This layer also controls single or multiple connections for each-end user application and directly communicates with both Presentation and transport layers.
9. Session Layer creates procedures for checkpointing followed by adjournment, restart and termination.
10. Session Layer uses checkpoints to enable communication sessions which are to be resumed from that particular checkpoint at which communication failure has occurred.
11. The session Layer is responsible for fetching or receiving data information from its previous layer (transport layer) and further sends data to the layer after it (presentation layer).

Q. 7 a: Write detailed note on “TCP vs UDP”.

Solution:

	TCP	UDP
Full form	It stands for **Transmission Control Protocol**.	It stands for **User Datagram Protocol**.
Type of connection	It is a connection-oriented protocol, which means that the connection needs to be established before the data is transmitted over the network.	It is a connectionless protocol, which means that it sends the data without checking whether the system is ready to receive or not.
Reliable	TCP is a reliable protocol as it provides assurance for the delivery of data packets.	UDP is an unreliable protocol as it does not take the guarantee for the delivery of packets.
Speed	TCP is slower than UDP as it performs error checking, flow control, and provides assurance for the delivery of	UDP is faster than TCP as it does not guarantee the delivery of data packets.
Header size	The size of TCP is 20 bytes.	The size of the UDP is 8 bytes.
Acknowledgment	TCP uses the three-way-handshake concept. In this concept, if the sender receives the ACK, then the sender will send the data. TCP also has the ability to resend the lost data.	UDP does not wait for any acknowledgment; it just sends the data.
Flow control mechanism	It follows the flow control mechanism in which too many packets cannot be sent to the receiver at the same time.	This protocol follows no such mechanism.
Error checking	TCP performs error checking by using a checksum. When the data is corrected, then the data is retransmitted to the receiver.	It does not perform any error checking, and also does not resend the lost data packets.
Applications	This protocol is mainly used where a secure and reliable communication process is required, like military services, web browsing, and e-mail.	This protocol is used where fast communication is required and does not care about the reliability like VoIP, game streaming, video and music streaming, etc.

Q. 7 b: Explain following application layer protocols:

- FTP
- SMTP
- DNS

Solution:

FTP

- FTP stands for File transfer protocol.
- FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.
- It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
- It is also used for downloading the files to computer from other servers.
- Objectives of FTP
- It provides the sharing of files.
- It is used to encourage the use of remote computers.
- It transfers the data more reliably and efficiently.

SMTP

- SMTP stands for Simple Mail Transfer Protocol.
- SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet is called Simple Mail Transfer Protocol.

- It is a program used for sending messages to other computer users based on e-mail addresses.
- It provides a mail exchange between users on the same or different computers, and it also supports:
- It can send a single message to one or more recipients.
- Sending message can include text, voice, video or graphics.
- It can also send the messages on networks outside the internet.
- The main purpose of SMTP is used to set up communication rules between servers. The servers have a way of identifying themselves and announcing what kind of communication they are trying to perform. They also have a way of handling the errors such as incorrect email address. For example, if the recipient address is wrong, then receiving server reply with an error message of some kind.

DNS

- An application layer protocol defines how the application processes running on different systems, pass the messages to each other.
- DNS stands for Domain Name System.
- DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
- DNS is required for the functioning of the internet.
- Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
- DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.
- For example, suppose the FTP site at XYZ had an IP address of 132.147.165.50, most people would reach this site by specifying ftp.XYZ.com. Therefore, the domain name is more reliable than IP address.
- DNS is a TCP/IP protocol used on different platforms. The domain name space is divided into three different sections: generic domains, country domains, and inverse domain.