20CB/ CS/DS/IT502

Hall Ticket Number:

III/IV B.Tech (Regular) DEGREE EXAMINATION

February,2023 **Common to CB,CS,DS & IT Branches**

Fifth Semester **Computer Networks**

Time: Three Hours **Maximum:** 70 Marks

Answer Question No. 1 Compulsorily. (14X1 = 14 Marks)

Answer ***ANY ONE*** *question from each Unit.* (4X14=56 Marks)

1.	a)	In what way you can summarize the purpose of layering.	CO1	L2	1M
	b)	Define Simplex, Half-Duplex and Full-Duplex.	CO1	L1	1M
	c)	Define computer Networks.	CO1	L1	1M
	d)	What is the need of Error Detection and Correction in Data Link Layer?	CO2	L2	1M
	e)	Define Flooding.	CO2	L3	1M
	f)	What is Stop-and-Wait Protocol?	CO2	L2	1M
	g)	What do you mean by slow start in TCP congestion?	CO3	L1	1M
	h)	Define QoS.	CO3	L1	1M
	i)	List the different phases used in TCP connection.	CO3	L1	1M
	j)	What are the metrics used by routing protocols?	CO3	L1	1M
	k)	What is SMTP?	CO4	L1	1M
	l)	Define congestion control.	CO4	L1	1M
	m)	How transport layer performs Duplication control?	CO4	L3	1M
	n)	What are the responsibilities of Application Layer?	CO4	L1	1M

Unit -I

2.	a)	How are headers and trailers attached when the data flows from the top layer to the bottom layer in the OSI reference model?	CO1	L1	7M
	b)	Compare and contrast between Synchronous and Asynchronous transmission using an example for each.	CO1	L3	7M

(OR)

3.	a)	Discuss in detail about the functions of network layer and transport layers with necessary diagrams.	CO1	L2	7M
	b)	What are the different applications of WAN and MAN? Explain.	CO1	L1	7M

Unit -II

4.	a)	Find CRC for the data polynomial $x^5+x^4+x^2+1$ with generator polynomial $x^3+ 1$.	CO2	L3	7M
	b)	Differentiate between adaptive and non-adaptive routing. Explain the working of 'Hierarchical Routing' using suitable topological structure and routing table.	CO2	L4	7M

(OR)

5.	a)	Compare between virtual circuits and Datagram subnets. Also discuss the effect of router failure in virtual circuits.	CO2	L1	7M
	b)	Explain how to control congestion in Datagram subnets.	CO2	L3	7M

Unit -III

6.	a)	How many networks can each IP address class A, B and C have? Also find the number of hosts per network in each given address class.	CO3	L4	7M
	b)	How is connection established in TCP ? Illustrate multiplexing in TCP.	CO3	L2	7M

(OR)

7.		Explain in detail about Leaky and Token bucket algorithms.	CO3	L3	14M

Unit -IV

8.	a)	Give the format of the UDP segment and TCP segment? Explain when UDP is preferred to TCP.	CO4	L1	7M
	b)	Explain the working of DNS.	CO4	L3	7M

(OR)

9.	a)	Differentiate between TCP and UDP	CO4	L2	7M
	b)	Discuss in detail about the connection establishment and release in TCP.	CO4	L3	7M

1. a) In what way you can summarize the purpose of layering.

The reasons for why we need layered network model is, let us assume that we have all functionalities of computer network in one layer, if any **changes** occurs in anywhere of the system is that change affect the entire system. And **identifying the problem** is also very critical.

b) Define Simplex, Half-Duplex and Full-Duplex.

Data in a simplex channel is always one way. Simplex channels are not often used because it is not possible to send back error or control signals to the transmit end.
A half-duplex channel can send and receive, but not at the same time. Only one end transmits at a time.
Data can travel in both directions simultaneously. There is no need to switch from transmit to receive mode like in half duplex.

c) Define computer Networks.

A computer network is a number of computers (also known as nodes) connected by some communication lines. (Or) A network is a collection of autonomous systems connected together by using some connecting devices (hub, switch etc….) or communication lines. The inter connection of these networks by using interconnecting devices (bridge, gateway etc….) was called internet.

d) What is the need of Error Detection and Correction in Data Link Layer?

Error control in data link layer is the process of detecting and correcting data frames that have been corrupted or lost during transmission. In case of lost or corrupted frames, the receiver does not receive the correct data-frame and sender is ignorant about the loss.

e) Define Flooding.

Flooding is a non-adaptive routing technique following this simple method: when a data packet arrives at a router, it is sent to all the outgoing links except the one it has arrived on.

f) What is Stop-and-Wait Protocol?

The data that sender wants to send, he sends the data to the receiver. After sending the data, he stops and waits until he receives the acknowledgment from the receiver. The stop and wait protocol is a flow control protocol where flow control is one of the services of the data link layer.

g) What do you mean by slow start in TCP congestion?

TCP slow start is a congestion-avoidance algorithm that balances the speed of a network connection. A slow start gradually increases the amount of data transmitted until it finds the network's maximum carrying capacity.

h) Define QoS.

it is not only the matter of providing speedy services, it is also matter of providing qualitative services. The goal of QOS is improve the overall performance of a network. This was achieved by good design of network and protocols.

i) List the different phases used in TCP connection.

SYN and ACK flags are used in connection established phase of different request and replay packets. for **request** SYN=1 and ACK=0

- for **replay** SYN=1 and ACK=1
- for **acknowledgement** SYN=0 and ACK=1

j) What are the metrics used by routing protocols?

Distance, number of hops, or estimated transit time.

k) What is SMTP?

Send mail transfer protocol. Protocols that define the formatting, delivery and storage of electronic mail messages on TCP/IP networks.

l) Define congestion control.

Congestion control is a mechanism that controls data flow when congestion actually occurs. It controls data entering in to a network such that the network can handle the traffic within the network.

m) How transport layer performs Duplication control?

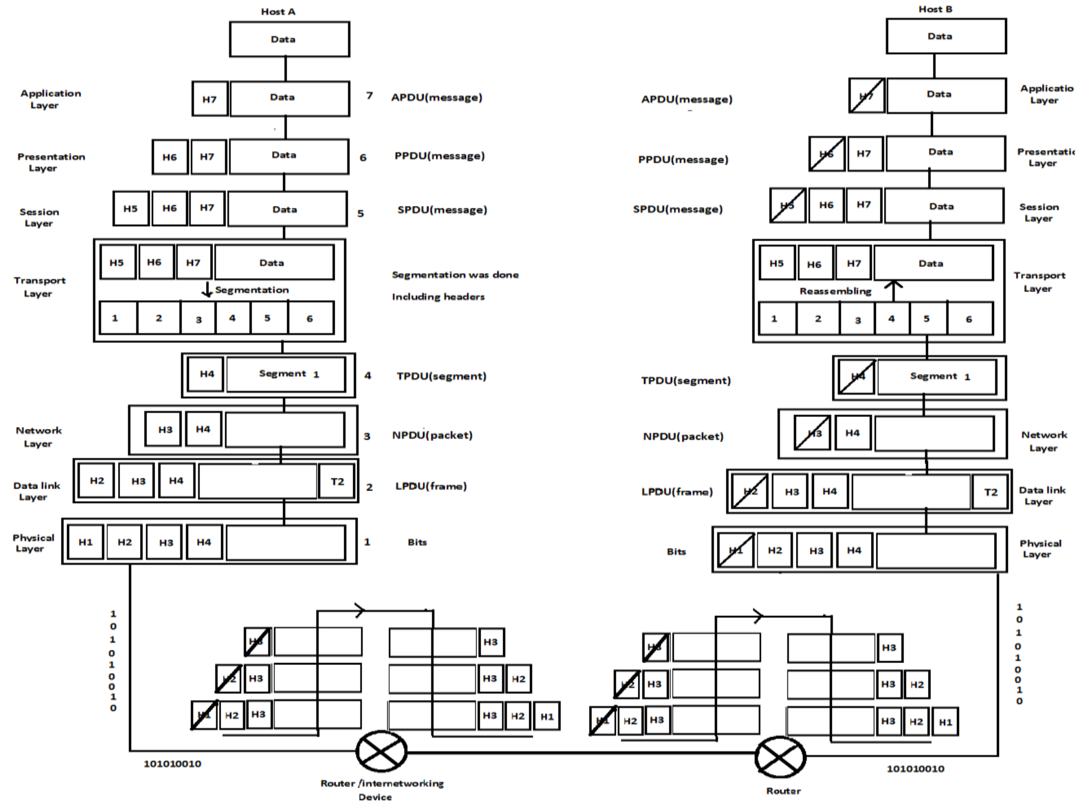
The transport layer ensures that no duplicate data is delivered to the destination. Sequence numbers are used to detect missing packets, as well as to identify and delete duplicate segments by the receiver.

n) What are the responsibilities of Application Layer?

Application layer is responsible for displaying data and images to the user in a human-recognizable format and it is done with help of interface with the presentation layer below it. And application layer services initiate the data transfer

2. a) How are headers and trailers attached when the data flows from the top layer to the bottom layer in the OSI reference model? 7M

4. Working of OSI reference model:



Step 1: whenever we open our browser, login onto web email client (Gmail, yahoo etc) by using web browser and at the moment when we attach one doc file of 512 kb where application layer comes into picture. And application layer adds its header (H7).

Step 2: in data link layer the 512 kb message is compressed into 300 kb and encryption and decryption was done if it needs any security. And add its header (H6) to the data coming from the above layer (application layer). And send that data to transport layer.

Step 3: in session layer add session header (H5) to the message coming from the above layer. And send to the next layer. Session layer is responsible for establish and maintain the sessions.

Step 4: the transport layer divides 300 kb of data in to small **segments** and transfers the each segment. We already know that transport layer responsibility is process to process delivery. For that add transport layer header (H4) to each segments. Transport layer header is given below.

Step 5: where in network layer IP header (H3) was added to the segment coming from the above layer (transport layer). Here the PDU is known as **packet**. We already aware of network layer is responsible for routing and host to host delivery this done by using IP header.
Step 6: in data link add header (H2) to the packet coming from the above layer. That is known as **frame**. Data link layer is responsible for hop to hop delivery for that it uses 48-bit MAC address. And send frame to the next layer i.e application layer.
Step 7: physical layer responsibility is converts each and every frame into bits and send that binary data to the router in the local network (also called **default gateway**).Now the data is entered into the network, by using MAC address (hop to hop), IP address (host to host) it reaches the other communication end point.

Step 8: now the physical layer responsibility on the receiver side is convert that binary information back to the original form. And send to the upper layer.

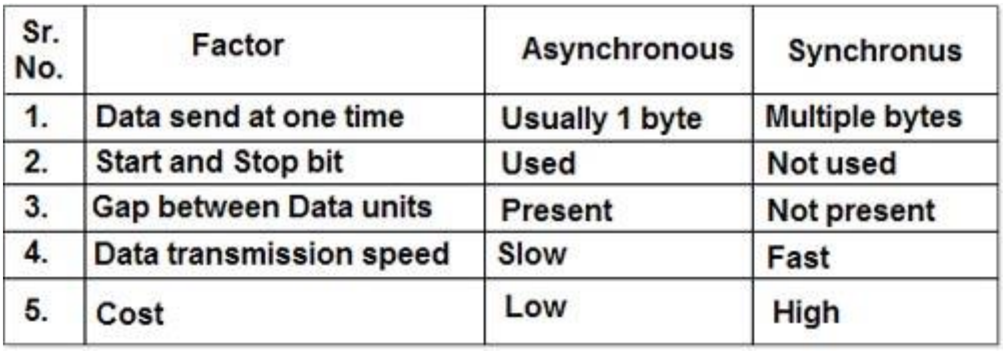
Step 9: in data link layer and network layer, the exactly reverse process was done in receiver side.

Step 10: the receiver side transport layer is responsible for reassembling of segments into a message. Reassembling was done based up on the **sequence numbers (32-bit)**. That's way TCP is called reliable protocol.

Step 11: in presentation layer the 300 kb data is again expansion back to the original format i.e 512 kb. And removes its header and send to application layer.

Step 12: now application layer shows the attached file content in the host B.

b) Compare and contrast between Synchronous and Asynchronous transmission using an example for each.



Sr. No.	Factor	Asynchronous	Synchronus
1.	Data send at one time	Usually 1 byte	Multiple bytes
2.	Start and Stop bit	Used	Not used
3.	Gap between Data units	Present	Not present
4.	Data transmission speed	Slow	Fast
5.	Cost	Low	High

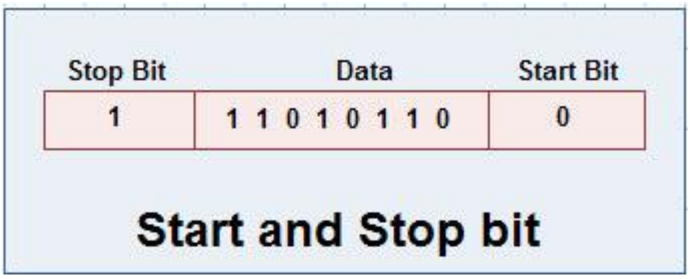
Asynchronous Transmission

• Asynchronous transmission sends only one character at a time where a character is either a letter of the alphabet or number or control character *i.e.* it sends one byte of data at a time.

• Bit synchronization between two devices is made possible using start bit and stop bit.

• Start bit indicates the beginning of data *i.e.* alerts the receiver to the arrival of new group of bits. A start bit usually 0 is added to the beginning of each byte.

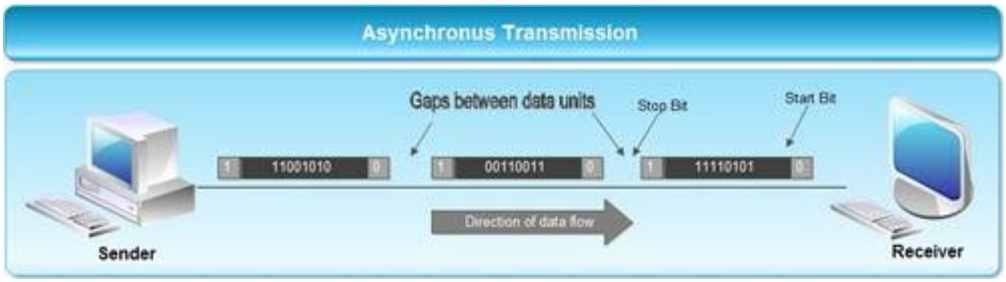
• Stop bit indicates the end of data *i.e.* to let the receiver know that byte is finished, one or more additional bits are appended to the end of the byte. These bits, usually 1s are called stop bits.



• Addition of start and stop increase the number of data bits. Hence more bandwidth is consumed in asynchronous transmission.

• There is idle time between the transmissions of different data bytes. This idle time is also known as Gap

• The gap or idle time can be of varying intervals. This mechanism is called Asynchronous, because at byte level sender and receiver need not to be synchronized. But within each byte, receiver must be synchronized with the incoming bit stream.

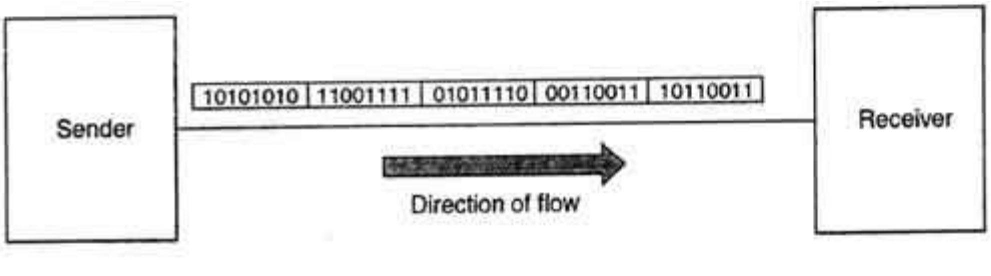


Synchronous Transmission

• Synchronous transmission does not use start and stop bits.

• In this method bit stream is combined into longer frames that may contain multiple bytes.

• There is no gap between the various bytes in the data stream.



Synchronous Transmission

• In the absence of start & stop bits, bit synchronization is established between sender & receiver by *'timing'* the transmission of each bit.

• Since the various bytes are placed on the link without any gap, it is the responsibility of receiver to separate the bit stream into bytes so as to reconstruct the original information.

• In order to receive the data error free, the receiver and sender operates at the same clock frequency.

(OR)

3. a) Discuss in detail about the functions of network layer and transport layers with necessary diagrams.
Network Layer-3.5M Transport Layer-3.5

<u>Network layer:</u> The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links).

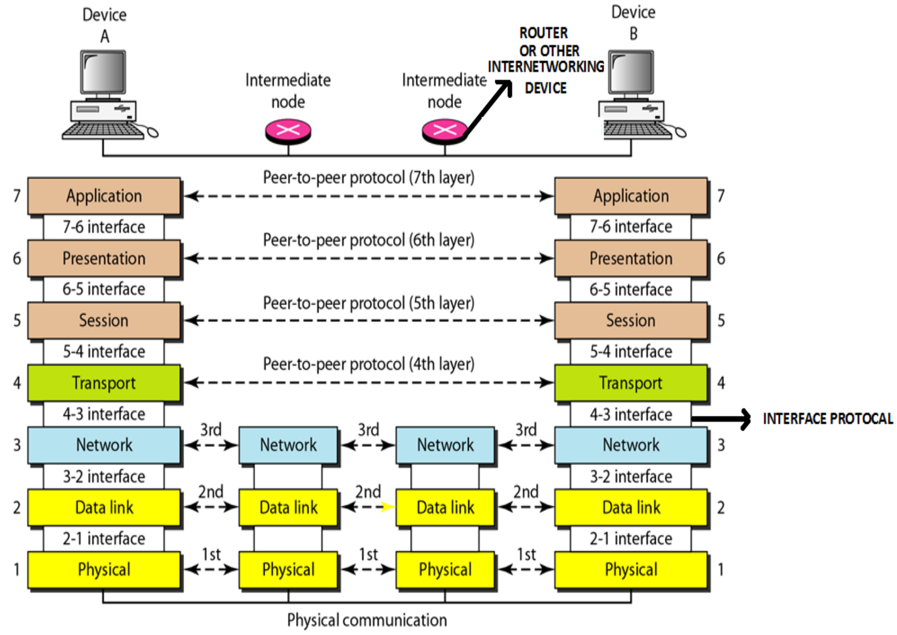
Whereas the data link layers over sees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination .The major function of the network layer is providing end to end communication by using IP address. In network layer The PDU is known as packet.

Functionalities:

Logical Addressing (IP address) systems: The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. That addressing system is known as logical addressing system (IP address).

Routing: When independent networks are connected to create internetworks (network of networks) the connecting devices (routers) route the packets to their final destination by finding the shortest distance between source and destination.

Congestion control: Higher rate of inputs to a router than outputs causes congestion, because the router buffer is full due to high speed of inputs. The results of congestion are Delays or Loss of packet.



<u>Transport layer:</u> transport layer offers process to process connection. In transport layer the data (PDU) coming from upper layers is divided into smaller PDU's and other side these smaller PDU's are again reassemble. Each PDU in transport layer is known as segment.

Functionalities:

Service point addressing: Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header must include a type of address called a service-point Address (or port address).The network layer gets each packet to the correct Computer; the transport layer gets the entire message to the correct processor of that computer.

Segmentation and reassembly: A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.

Flow control: Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performs end to end rather than across a single link.

Error control (checksum): Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to process rather than across a single hop.

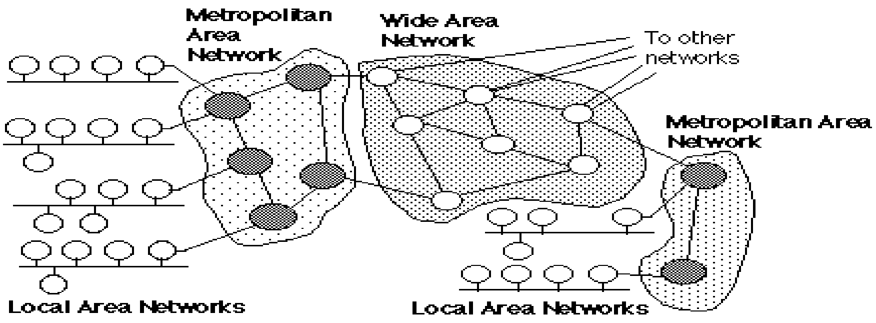
b) What are the different applications of WAN and MAN? Explain. 7M

MAN-3.5M WAN-3.5M

Metropolitan Area Network a network spanning physical larger area than a LAN but smaller than a WAN, such as a city, Your ISP are an examples of a MAN etc…

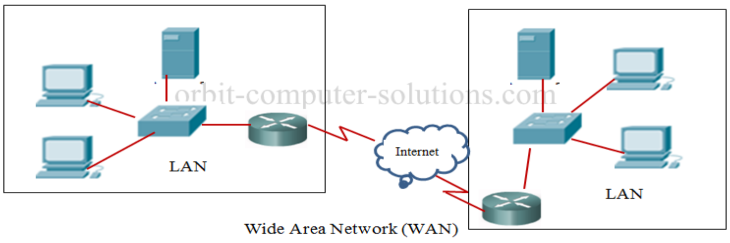
(or)

A Metropolitan Area Network (MAN) is a large computer network that spans a metropolitan area or campus. Its geographic scope falls between a WAN and LAN. MANs provide Internet connectivity for LANs in a metropolitan region, and connect them to wider area networks like the Internet.



Wide area networks (WANs) are used to connect LANs together by using a device called router. Typically, WANs are used when the LANs that must be connected are separated by a large distance.

WAN's connected networks in larger geographic areas, such as Florida, the United States, or the world.



Unit -II

4. a) Find CRC for the data polynomial $x^5+x^4+x^2+1$ with generator polynomial $x^3+ 1$.

b) Differentiate between adaptive and non-adaptive routing. Explain the working of 'Hierarchical Routing' using suitable topological structure and routing table.
adaptive and non-adaptive routing-2M 'Hierarchical Routing'-5M

S. No.	Adaptive Routing algorithm	Non-Adaptive Routing algorithm
1.	An adaptive algorithm involves routers for exchanging and updating router table data.	A non-adaptive algorithm involves a network administrator for the manual entry of the routing paths into the router.
2.	This algorithm creates a routing table based on network conditions.	Whereas this algorithm creates a static table in order to determine when to send packets and which node.
3.	This algorithm is used by dynamic routing.	Whereas this algorithm is used by static routing.
4.	In adaptive routing algorithm, the routing decisions are made based on network traffic and topology.	Whereas in a non-adaptive routing algorithm, the routing decisions are not made based on network traffic and topology.
5.	Adaptive routing algorithms are more complex as compared to non-adaptive routing algorithms in terms of complexity.	While non-adaptive routing algorithms are simple in terms of complexity.
6.	In adaptive routing algorithm, the routing decisions are not static tables.	While in non-adaptive routing algorithm, the routing decisions are static tables.

Hierarchical Routing: - • As networks grow in size, the router routing tables grow proportionally. Not only is router memory consumed by ever-increasing tables, but more CPU time is needed to scan them and more bandwidth is needed to send status reports about them.

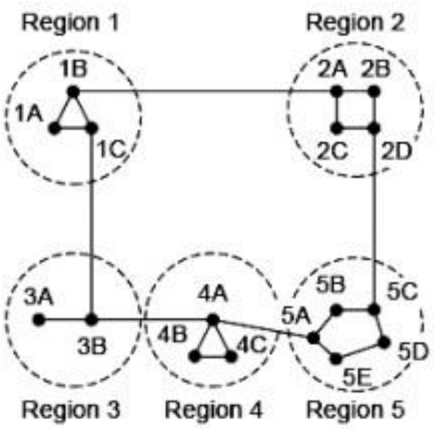
- At a certain point, the network may grow to the point where it is no longer feasible for every router to have an entry for every other router, so the routing will have to be done hierarchically, as it is in the telephone network. • When hierarchical routing is used.

In hierarchical routing, routers are classified in groups called regions. Each router has information about the routers in its own region and it has no information about routers in other regions. So, routers save one record in their table for every other region.

For huge networks, a two-level hierarchy may be insufficient hence, it may be necessary to group the regions into clusters, the clusters into zones, the zones into groups and so on.

Example

Consider an example of two-level hierarchy with five regions as shown in figure −



Let see the full routing table for router 1A which has 17 entries, as shown below −

Full Table for 1A

Dest.	Line	Hops
1A	-	-
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4

5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

When routing is done hierarchically then there will be only 7 entries as shown below −

Hierarchical Table for 1A

Dest.	Line	Hops
1A	-	-
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

Unfortunately, this reduction in table space comes with the increased path length.

Explanation

Step 1 − For example, the best path from 1A to 5C is via region 2, but hierarchical routing of all traffic to region 5 goes via region 3 as it is better for most of the other destinations of region 5.

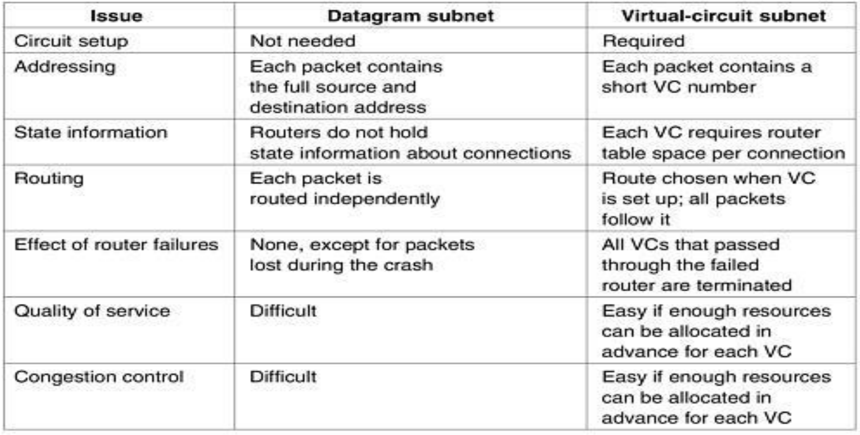
Step 2 − Consider a subnet of 720 routers. If no hierarchy is used, each router will have 720 entries in its routing table.

Step 3 − Now if the subnet is partitioned into 24 regions of 30 routers each, then each router will require 30 local entries and 23 remote entries for a total of 53 entries.

(OR)

5. a) Compare between virtual circuits and Datagram subnets. Also discuss the effect of router failure in virtual circuits.

virtual circuits and Datagram subnets-5M effect of router failure in virtual circuits-2M



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

The effect of router failure in virtual circuits:

Solution1: If any router is failed due to the congestion in a network then no new virtual circuits are set up until the problem was gone away.

Solution2: An alternative approach is to allow new virtual circuits but carefully route/establish all new virtual circuits around problem areas.

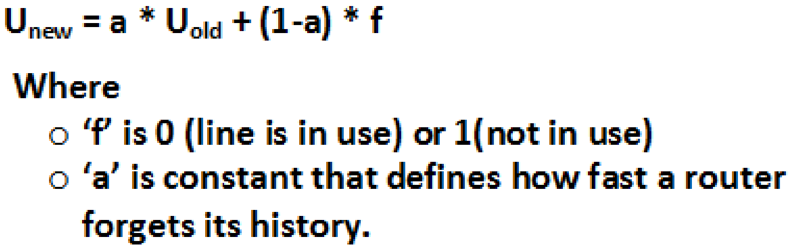
The working of this approach like this

- ○ **Step 1:** find out the congested routers in the network by using open loop mechanisms.
- ○ **Step 2:** construct a new subnet by eliminate those congested routers from the network.
- ○ **Step 3:** establish a new virtual connection.

b) Explain how to control congestion in Datagram subnets.

In datagram subnet congestion was finding out by using the characteristics routers like **average queue length**, Number **of packets that are timed-out and Average packet delay** and etc… and **performance** or **utilization** of outgoing lines of router.

- A router can identify utilization of its outgoing lines by using below formula



U_{new} = a * U_{old} + (1-a) * f

Where

- ○ **'f' is 0 (line is in use) or 1(not in use)**
- ○ **'a' is constant that defines how fast a router forgets its history.**

- Whenever the value of 'U' move above the threshold value then the router thinks that that link in warning state. Then the router chooses any one of the following mechanism to control congestion.
  - ○ Warning Bit
  - ○ Choke Packets
  - ○ Hop-by-Hop Choke Packets

The Warning Bit:

- In this mechanism a special **field** was used in header to indicate the warning state of resource.
- If the packet pass through the congested router, this field was filled with **1** else the value is **0**.
- When the packets reach its destination the value of this field was copied into the **ACK** and send to the source.
- As long as the router was in the warning state, it continued to set the warning bit, which meant that the source continued to get acknowledgements.

- If the source receives a warning state **ACK**, it reduces its transmission speed by ½ or ¼ or 1/8 and …… times.

Choke packets:

- In the previous mechanism/algorithm, it will take so much time to tell the source. To overcome that problem this mechanism introduces a new technique that is **just directly told to source.**
- **What is Choke packet?** A choke packet is a control packet produced at a congested node and transmitted back to a source node to reduce traffic flow.

Procedure:

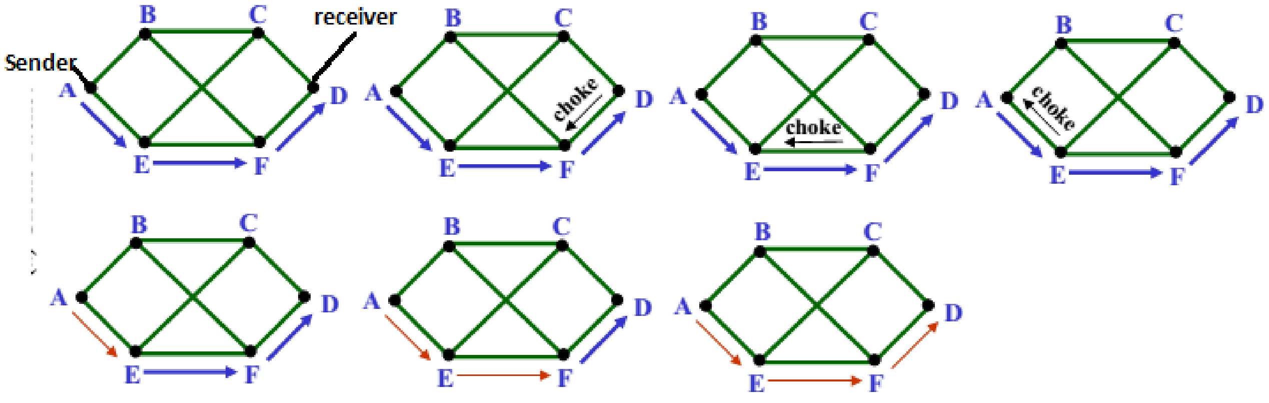
Step 1: router monitors the level of congestion around them.

Step 2: When congestion is present, they can send **choke packets** to the sender that say **`slow down'.**

Step 3: When the source host gets the choke packet, it is required to reduce flow sent to the specified destination by some percentage.

- In this mechanism sender listens the choke packets **periodically**. Because other packets aimed at the same destination are probably already under way and will generate yet more choke packets.

Example:



Advantages: Host sends as much data as it wants, the network informs it when it is sending too much.

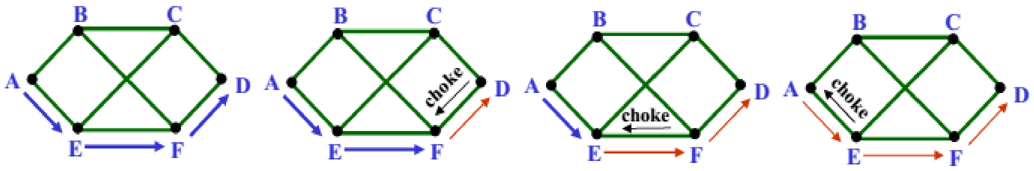
Disadvantages: Defining time that the sender slows down his speed is critical.

Hop by hop choke packets:

- If there is long distance exist between source and destination, sending choke packets to sender takes so much time. To overcome this problem the new technique was introduced in

- hop by **hop choke packet.**
- With **hop-by-hop choke packets** each **intermediate router also reacts on a choke packet** by reducing its sending rate. For that it needs sufficient buffers to store the packets which still come in at a too high rate.

Example:



6. a) How many networks can each IP address class A, B and C have? Also find the number of hosts per network in each given address class.

Class A, B, and C are used by the majority of devices on the Internet.

Classes are defined by leading bits of the first octet:

- 0 - Class A (128 networks)
- 10 - Class B (16384 networks)
- 110 - Class C (2097152 networks)
- 1110 - Class D (Multicast)
- 1111 - Class E

Class A: Public IP Range: 1.0.0.0 to 127.0.0.0

- First octet value range from 1 to 127
- Subnet Mask: 255.0.0.0 (8 bits)
- Number of Networks: 126
- Number of Hosts per Network: 2^{24} equals to 16,777,214

Class B: Public IP Range: 128.0.0.0 to 191.255.0.0

- First octet value range from 128 to 191
- Number of Networks:2^{14} equals to 16,382
- Number of Hosts per Network: 2^{16} equals to 65,534

Class C:Public IP Range: 192.0.0.0 to 223.255.255.0

- First octet value range from 192 to 223
- Number of Networks:2^{21} equals to 2,097,150
- Number of Hosts per Network:2^{8}

b) How is connection established in TCP? Illustrate multiplexing in TCP. 7M

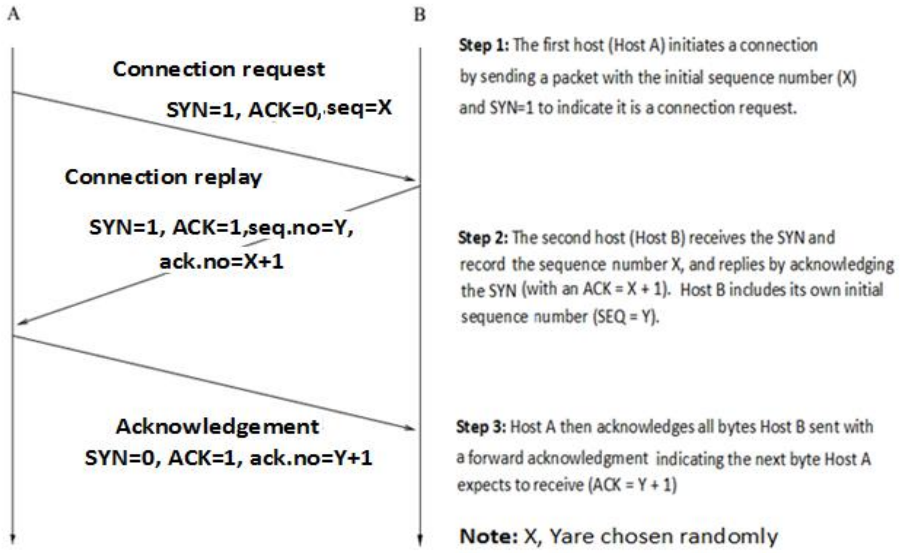
connection establishment-3.5M Multiplexing 3.5M

To use reliable transport services, processes must establish a connection-oriented session with one another. Connection establishment is performed by using a "**three-way handshake (**SYN, SYN-ACK, and ACK)" mechanism.

Three-way handshake synchronizes both ends of a connection by allowing both sides to agr **initial sequence numbers**.

- This mechanism also guarantees that both sides are ready to transmit data and know that the ot is ready to transmit as well.
- For establishing a connection, one side host of communication wait for an incoming conne executing LISTEN and ACCEPT primitives. And other side host connect to it by ex CONNECT primitive.

Procedure for TCP connection establishment in general case



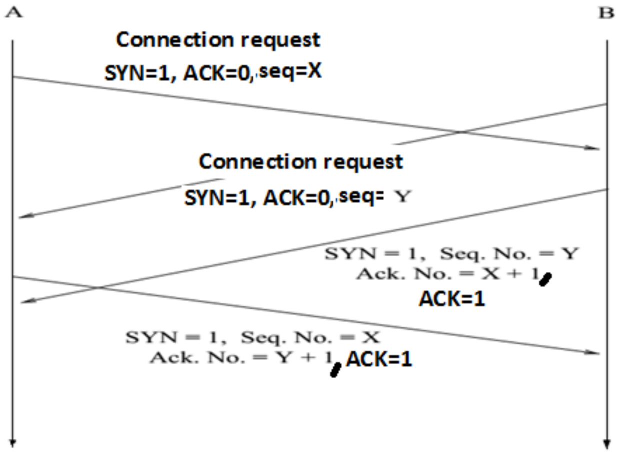
Step 1: The first host (Host A) initiates a connection by sending a packet with the initial sequence number (X) and SYN=1 to indicate it is a connection request.

Step 2: The second host (Host B) receives the SYN and record the sequence number X, and replies by acknowledging the SYN (with an ACK = X + 1). Host B includes its own initial sequence number (SEQ = Y).

Step 3: Host A then acknowledges all bytes Host B sent with a forward acknowledgment indicating the next byte Host A expects to receive (ACK = Y + 1)

Note: X, Yare chosen randomly

Then what happens at both two hosts simultaneously attempt to establish a connection between the s sockets. This situation was called **call collision** is explain below.



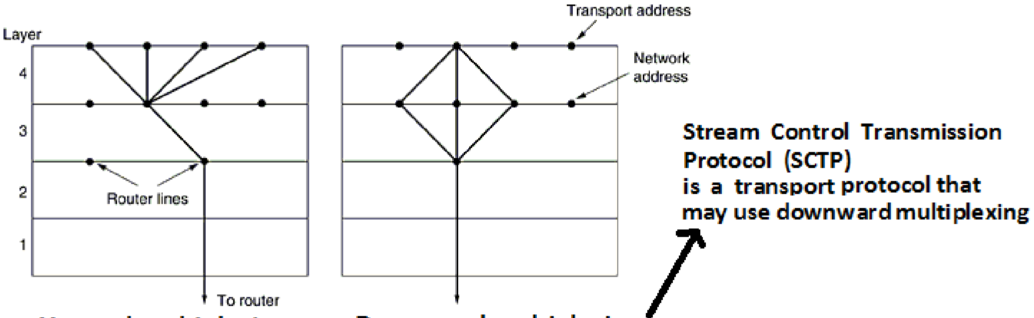
- The result of these events is that just one connection is established, not two because connect identified by their end points. If the first setup results in a connection identified by(x, y) second one does too, only one table entry is made, namely, for (x, y).

Multiplexing:

The process of combining the information coming from multiple channels and transmit over a shared channel is known as **multiplexing**.

- It plays a role in transport layers of internet architecture, based on usage multiplexing were divided into two types in transport layer.
  - Upward multiplexing.
  - Downward multiplexing.
- **Upward multiplexing:** Now days, each and every host supports the multitasking. I.e. each host may run multiple processes at a time; each one was identified by a TSAP (port number). And each host has single IP address [NSAP] (except multi home devices).
  When a TPDU comes in from different process, and all of them are must transmit to destination in a single channel. The process of combining data from different processes into a single channel is known as **upward multiplexing.**

Diagram:


Transport address
Layer
4
3
2
1
Network address
Router lines
To router
Stream Control Transmission Protocol (SCTP) is a transport protocol that may use downward multiplexing

- Upward multiplexing Downward multiplexing

Downward multiplexing: is the inverse scenario where a single network connection cannot handle the traffic from the transport layer process. By dividing the traffic among different network connections, it is possible to get better throughput. This mechanism is known as **downward multiplexing.**

(OR)

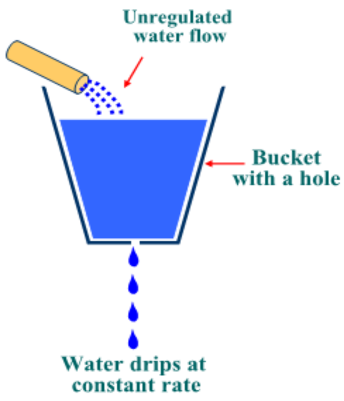
7. Explain in detail about Leaky and Token bucket algorithms. 14M

Each algorithm 7M

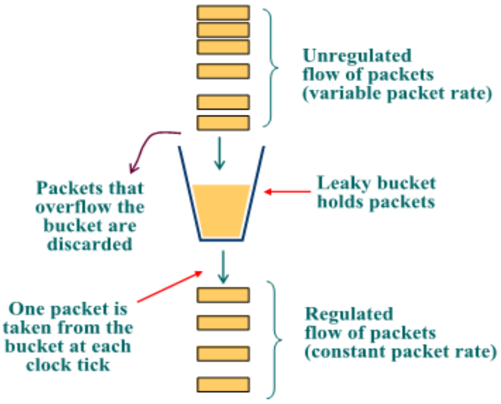
Leaky Bucket Algorithm/ peak rate limiter:

- The Leaky Bucket Algorithm used to control rate in a network. It is implemented as a single-server queue with constant service time. It was proposed a 19th century networking engineer by **Turner**.
- One day evening turner sit on his house balcony, his father is cleaning his motor cycle with a bucket of water and some cloth. That bucket has a hole on lower part of it. The water was leaking at a constant rate, after some time the bucket was empty because of leakage. And his mother fill that bucket with water by using other bucket (it has better storage capacity) at the end of filling process the water start spills over the sides of bucket.
- From that situation he observe two important points
  - The water was leaking at a constant rate
  - Water start spills over the sides of bucket when the bucket is full.
- By using those two points he implements a new algorithm.

Diagram:



A leaky bucket with water


Unregulated flow of packets (variable packet rate)
Packets that overflow the bucket are discarded
Leaky bucket holds packets
One packet is taken from the bucket at each clock tick
Regulated flow of packets (constant packet rate)

A leaky bucket with packets

Algorithm:

- ○ **Step 1:** Does nothing when input is idle.
- ○ **Step 2:** When a packet arrives, if buffer is full then discard packet. Else append to the buffer.
- ○ **Step 3:** At every **clock tick**, one packet is transmitted (unless the queue is empty).

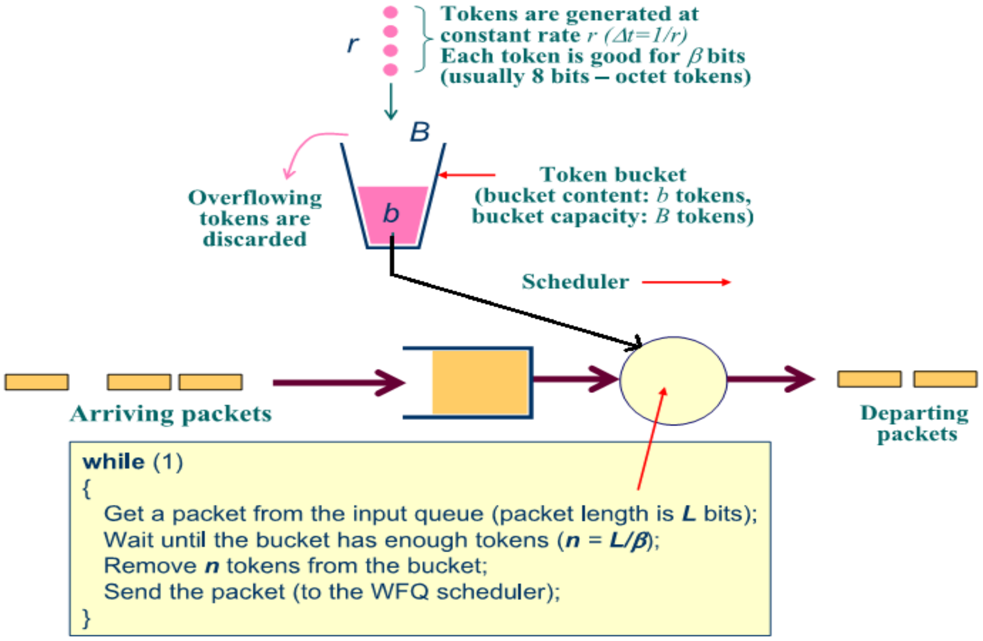
- **Advantages:** control data rate in a network.
- **Disadvantage**: If data sending too fast, data is dropped.
- If all packets are of the same size the algorithm works as described in above.
- If packets have variable size, use number of bytes per clock-tick **For example** assumes the rule is 1024 bytes per clock-tick for every clock-tick the source can send: a single 1024 byte packet, or two 512 bytes packets, and etc ... it is also called **byte-counting leaky bucket.**

Token bucket algorithm:

- Leaky bucket algorithm does not allow sending **burst of packets**, but only at a specified

  rate. If there is no traffic for a certain period of time, the amount of unused bandwidth cannot be used for later packets; this is achieved by using a token bucket algorithm.

Algorithm:


r
Tokens are generated at constant rate r (Δt=1/r)
Each token is good for β bits (usually 8 bits – octet tokens)
B
b
Overflowing tokens are discarded
Token bucket (bucket content: b tokens, bucket capacity: B tokens)
Scheduler
Arriving packets
Departing packets

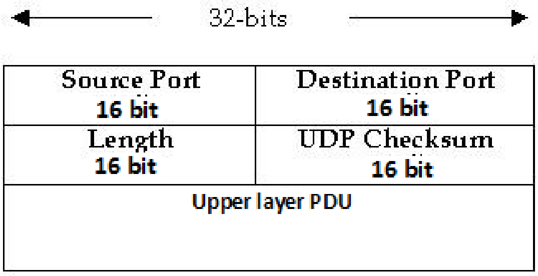
```
while (1)
{
   Get a packet from the input queue (packet length is L bits);
   Wait until the bucket has enough tokens (n = L/β);
   Remove n tokens from the bucket;
   Send the packet (to the WFQ scheduler);
}
```

Unit -IV

8. a) Give the format of the UDP segment and TCP segment? Explain when UDP is preferred to TCP. 7M

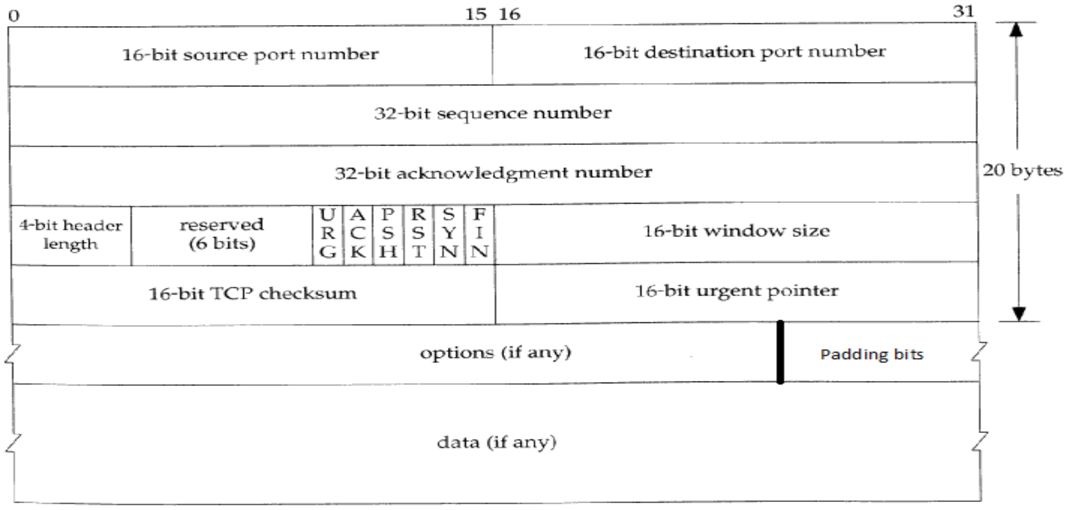
UDP segment and TCP segment 5M UDP than TCP -2M

UDP Segment header:



UDP segment structure

TCP Segment Header:



TCP and UDP are the most widely-used communication protocols in the Internet protocol suite. One ensures the data you send is received accurately. The other transfers data quickly. Whether an application uses TCP vs. UDP depends on the relative importance of accuracy vs. speed.
UDP benefits applications that need to receive data quickly even if accuracy suffers. This is why real-time applications like audio and video streaming will often use UDP. **Transport layer also provides unreliable services by using UDP**, but for limited applications like streaming, multimedia applications. An easy way to understand the difference is to consider ways to distribute video. When downloading movies, a media app would use TCP. The priority here is delivering the file accurately to ensure correct playback. When streaming video, however, accuracy is less important than continuity. UDP ensures that data arrives at the streamer quickly.

b) Explain the working of DNS. 7M

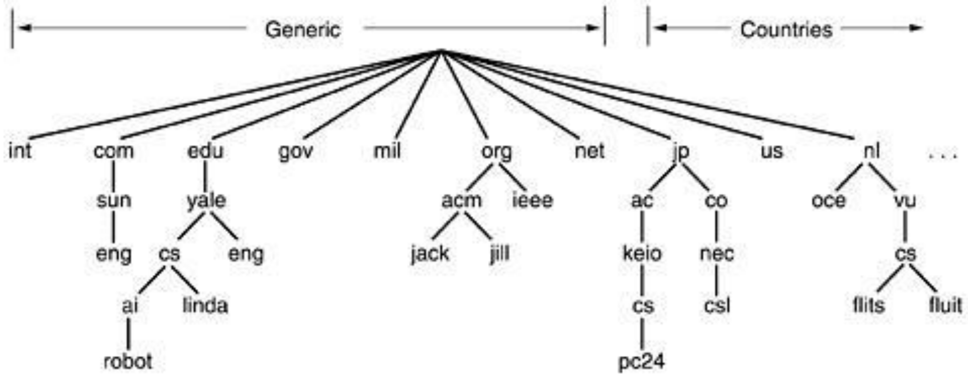
- The **Domain Name System** (aka DNS) is used to resolve human-readable hostnames like **www.Dyn.com** into machine-readable **IP addresses** like ***204.13.248.115.***

- DNS is like a phone book for the Internet. If you know a person’s name but don’t know their telephone number, you can simply look it up in a phone book. DNS provides this same service to the Internet.
- When you visit *http://dyn.com* in a browser, your computer uses DNS to retrieve the website’s IP address of *204.13.248.115*. Without DNS, you would only be able to visit our website (or any website) by visiting its IP address directly, such as *http://204.13.248.115*.

The DNS Name Space

- Conceptually, the Internet is divided into over 200 top-level **domains**, where each domain covers many hosts.
- Each **domain** is partitioned into **subdomains,** and these are further partitioned, and so on. All these domains can be represented by a **tree.**
- The leaves of the tree represent domains that have no subdomains (but do contain machines, of course).
- A leaf domain may contain a single host, or it may represent a company and contain thousands of hosts.

Fig. A portion of the Internet domain name space.



- The top-level domains come in two flavors: **generic and countries.**
- The original **generic domains** were ***com*** *(commercial)*, ***edu*** (educational institutions), ***gov*** (the U.S. Federal Government), ***int*** (certain international organizations), ***mil*** (the U.S. armed forces), ***net*** (network providers), and ***org*** (nonprofit organizations).

DNS Working Procedure:

Step 1: Request information

- The process begins when you ask your computer to resolve a hostname, such as visiting *http://dyn.com*. The first place your computer looks is its local DNS cache, which stores information that your computer has recently retrieved.
- If your computer doesn't already know the answer, it needs to perform a **DNS query** to find out.

Step 2: Ask the recursive DNS servers

- If the information is not stored locally, your computer queries (contacts) your ISP's **recursive DNS servers**. These specialized computers perform the legwork of a DNS query on your behalf.
- **Recursive servers** have their own caches, so the process usually ends here and the

information is returned to the user.

Step 3: Ask the root name servers

- If the recursive servers don't have the answer, they query the **root name servers**.
- A **name server** is a computer that answers questions about domain names, such as IP addresses. The thirteen root name servers act as a kind of telephone switchboard for DNS. They don't know the answer, but they can direct our query to someone that knows where to find it.

Step 4: Ask the TLD name servers

- The root name servers will look at the first part of our request, reading from right to left — *www.dyn.**com*** — and direct our query to the **Top-Level Domain (TLD) name servers** for *.com*. Each TLD, such as *.com*, *.org*, and *.us*, have their own set of name servers, which act like a receptionist for each TLD. These servers don't have the information we need, but they can refer us directly to the servers that *do* have the information.

Step 5: Ask the authoritative DNS servers

- The TLD name servers review the next part of our request — *www.**dyn.com*** — and direct our query to the name servers responsible for this *specific* domain.
- These **authoritative name servers** are responsible for knowing all the information about a specific domain, which are stored in **DNS records**.
- There are many types of records, which each contain a different kind of information. In this example, we want to know the IP address for *www.dyndns.com*, so we ask the authoritative name server for the **Address Record (A)**.

Step 6: Retrieve the record

- The recursive server retrieves the A record for *dyn.com* from the authoritative name servers and stores the record in its local cache. If anyone else requests the host record for *dyn.com*, the recursive servers will already have the answer and will not need to go through the lookup process again. All records have a **time-to-live** value, which is like an expiration date. After a while, the recursive server will need to ask for a new copy of the record to make sure the information doesn't become out-of-date.

Step 7: Receive the answer

- Armed with the answer, recursive server returns the A record back to your computer.

Your computer stores the record in its cache, reads the IP address from the record, and then passes this information to your browser. The browser then opens a connection to the webserver and receives the website.

(OR)

9. a) Differentiate between TCP and UDP 7M

Any 7 relevant and suitable differences

Basis	**Transmission control protocol (TCP)**	**User datagram protocol (UDP)**

Type of Service	TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram-oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast types of network transmission.
Reliability	TCP is reliable as it guarantees the delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
Error checking mechanism	TCP provides extensive error-checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error checking mechanism using checksums.
Acknowledgment	An acknowledgment segment is present.	No acknowledgment segment.
Sequence	Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in order at the receiver.	There is no sequencing of data in UDP. If the order is required, it has to be managed by the application layer.
Speed	TCP is comparatively slower than UDP.	UDP is faster, simpler, and more efficient than TCP.
Retransmission	Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in the User Datagram Protocol (UDP).
Header Length	TCP has a (20-60) bytes variable length header.	UDP has an 8 bytes fixed-length header.
Weight	TCP is heavy-weight.	UDP is lightweight.
Handshaking Techniques	Uses handshakes such as SYN, ACK, SYN-ACK	It’s a connectionless protocol i.e. No handshake
Broadcasting	TCP doesn’t support Broadcasting.	UDP supports Broadcasting.

Protocols	TCP is used by HTTP, HTTPs, FTP, SMTP and Telnet.	UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP.
Stream Type	The TCP connection is a byte stream.	UDP connection is message stream.
Overhead	Low but higher than UDP.	Very low.

b) Discuss in detail about the connection establishment and release in TCP. 7M

connection establishment 3.5M and connection release 3.5M

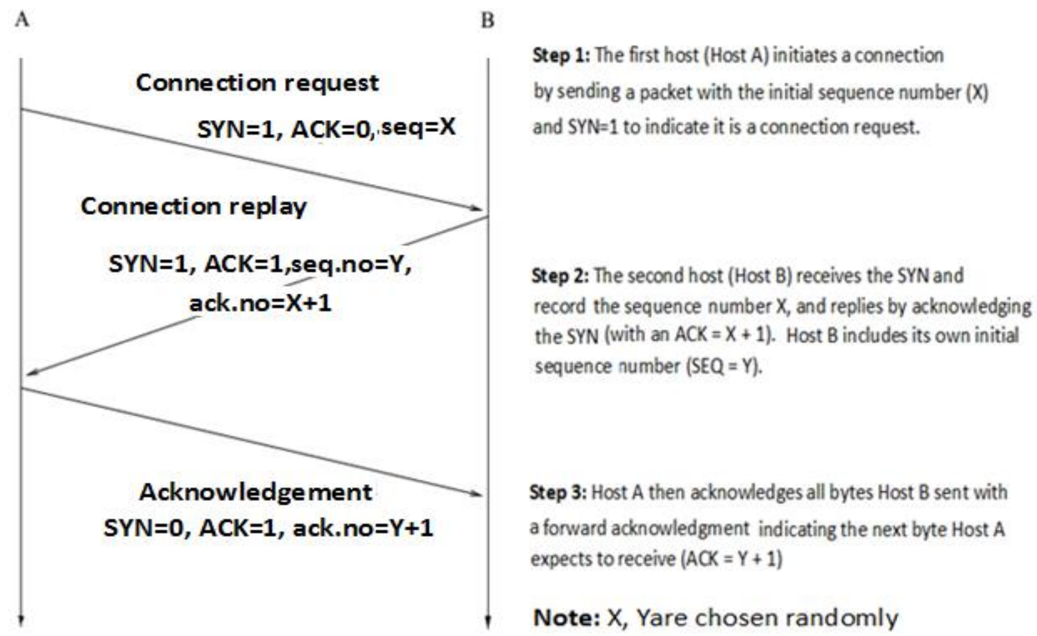
TCP connection establishment

To use reliable transport services, processes must establish a connection-oriented session with one another. Connection establishment is performed by using a "**three-way handshake (**SYN, SYN-ACK, and ACK)" mechanism.

Three-way handshake synchronizes both ends of a connection by allowing both sides to agr **initial sequence numbers**.

- This mechanism also guarantees that both sides are ready to transmit data and know that the ot is ready to transmit as well.
- For establishing a connection, one side host of communication wait for an incoming conne executing LISTEN and ACCEPT primitives. And other side host connect to it by ex CONNECT primitive.

Procedure for TCP connection establishment in general case



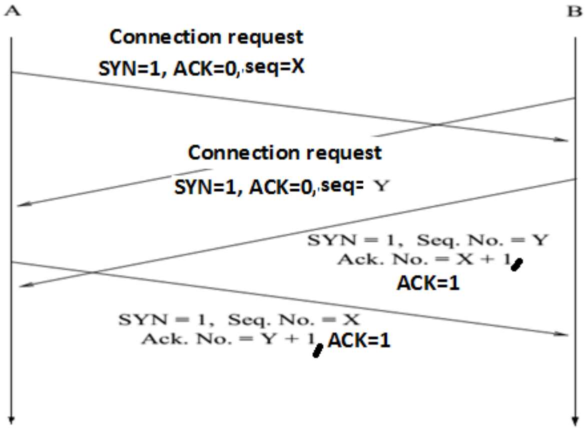
Step 1: The first host (Host A) initiates a connection by sending a packet with the initial sequence number (X) and SYN=1 to indicate it is a connection request.

Step 2: The second host (Host B) receives the SYN and record the sequence number X, and replies by acknowledging the SYN (with an ACK = X + 1). Host B includes its own initial sequence number (SEQ = Y).

Step 3: Host A then acknowledges all bytes Host B sent with a forward acknowledgment indicating the next byte Host A expects to receive (ACK = Y + 1)

Note: X, Yare chosen randomly

Then what happens at both two hosts simultaneously attempt to establish a connection between the sa sockets. This situation was called **call collision** is explain below.

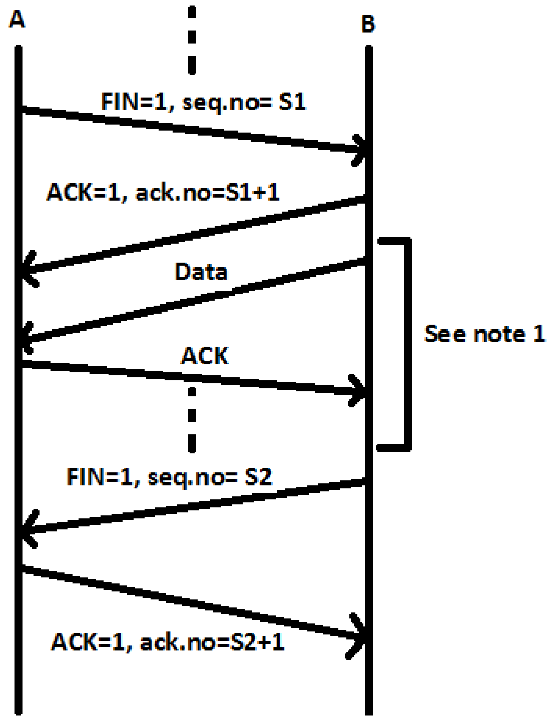


The result of these events is that just one connection is established, not two because connection identified by their end points. If the first setup results in a connection identified by(x, y) and the se one does too, only one table entry is made, namely, for (x, y).

TCP Connection Release:

TCP connection is a full duplex connection i.e. two half duplex connections one in each direction. So at the time of terminating, each connection was terminated separately.

- To release a connection, either party can send a segment with the FIN=1.
- Normally, **four TCP segments** are needed to release a connection.
  - One FIN and one ACK form initiator side.
  - One FIN and one ACK form other side.



Step 1: the initiator of the connection termination, sends a segment, that consist of FIN=1, and some sequence number.

Step 2: the receiver sends an acknowledgement by sending the segment that consists of ACK=1, ack.no= S1+1.

Step 3: the other side process (B) transmits its data and wants to terminate the connection by sending a segment that consists of FIN=1, seq.no=S2.

Step 3: finally the process A needs to acknowledge that request by sending an acknowledgement segment ACK=1, ack.no=S2+1.

Note 1: the connection was terminated in direction means it can't transfer data anymore but it receives data from other end.

It is possible to reduce the number of segments into three. For the first ACK and the second FIN to be contained in the same segment. Of course it is suffers from the problems like **“two man army problem”**. By using **timers** we solve this problem, but this solution is not perfect. Let us assume that, if a response to a FIN is not forthcoming within timeout, the sender of the FIN releases the connection. The other side will eventually notice that nobody seems to be listening to it anymore and will time out as well. The fact that a perfect solution is theoretically impossible, it will have to do. In practice, problems rarely arise.