F – 54302

Register No. | | | | | | | | |

BE Degree Examination December 2022

Fifth Semester

Computer Science and Engineering

20CST51 – COMPUTER NETWORKS

(Regulations 2020)

Time: Three hours Maximum: 100 marks

Answer all Questions

Part – A (10 × 2 = 20 marks)

1. Define processing delay and queuing delay. [CO1,K1]
2. Differentiate between packet switching and circuit switching. [CO1,K2]
3. List two Internet applications and the application layer protocols that they use. [CO2,K1]
4. Define handshaking. [CO2,K1]
5. Consider sending a 3000 byte datagram into a link that has a MTU of 500 bytes. Suppose the original datagram in stamped with the ID 422. How many fragments are generated? [CO3,K2]
6. State the significance of selective repeat protocol. [CO3,K1]
7. Mention the important of CIDR addressing. [CO4,K1]
8. Recall the role of DHCP in networking applications. [CO4,K1]
9. State the purpose of ARP in a network. [CO5,K1]
10. Draw the Ethernet frame structure. [CO5,K1]

Part – B (5 × 16 = 80 marks)

11. a. i) Consider two hosts A and B, connected by a single link of rate R bps. suppose that the two hosts are separated by 'm' meters and the propagation speed along the link is s meters/sec. Host A is to send a packet of size L bits to Host B. Answer the following: (8) [CO1,K3]

1) Express propagation delay d_{prop}, in terms of 'm' and 's'

2) Calculate the transmission time of a packet, 'd_{trans}' in terms of L and R.

3) Give the expression for end-to-end-delay (Ignore processing and queuing delay)

4) Suppose Host A begins to transmit at time t = 0. At time t = d_{trans}, where is the last bit of the packet?

5) Suppose s = 2.5 * 10^8, L = 2000 bytes and R = 10 Mbps. Find the distance 'm' so that d_{prop} equals d_{trans}.

ii) Classify the different types of access networks. Provide a brief comparison of them. (8) [CO1,K2]

(OR)

b. i) Draw the IP protocol stack for a typical network. Highlight the role of each layer in the protocol stack. (8) [CO...

ii) Suppose two hosts, A and B are separated by 20,000 kms and are connected by a direct link of R = 5 Mbps. Suppose the propagation speed over the link is $2.5 * 10^8$ meters/sec. (8) [CO1,K...

1) Calculate the bandwidth-delay product, R x d_{prop}.
2) Consider sending a file of 8,00,000 bits from Host A to Host B. suppose the file is sent continuously as one large message. Find the maximum of bits that will be in the link at any given time?
3) Find the width (in meters) of a bit in the link.

12. a. i) Write a simple TCP program for a server that accepts of input from a client and prints the lines onto the server's standard output. (10) [CO2,K3]

ii) With a neat sketch, list the steps involved when a DNS server redirects a user's request to a CDN server. (6) [CO2,K1]

(OR)

b. i) Support user A, with a web-based e-mail account like Gmail, sends a message to user B, who accesses A's mail using IMAP mail server. Show diagrammatically how the message moves from A to B List the application layer protocols that are used to move the message between A and B along with their roles. (10) [CO2,K3]

ii) Enumerate the steps involved while transferring a web page from a server to a client in case of non persistent connections. (6) [CO2,K1]

13. a. i) Draw the structure of TCP header. Provide a brief summary on the significance of each field in the TCP header. (8) [CO3,K2]

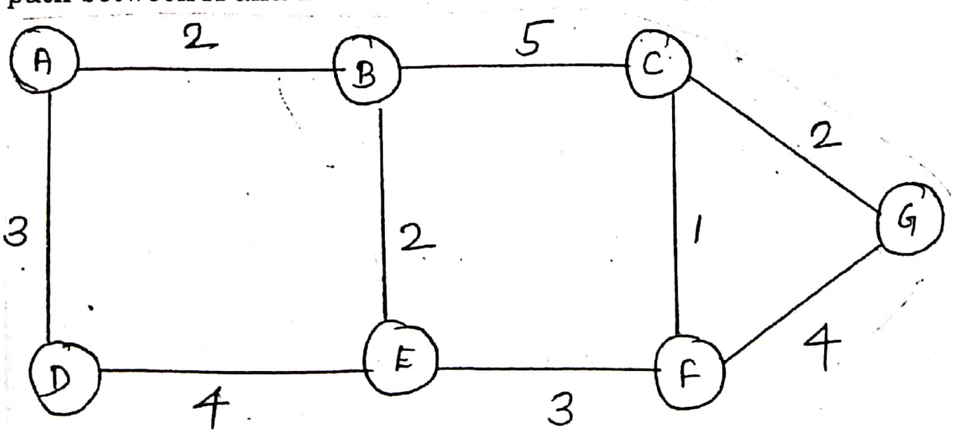
ii) Identify the components of the congestion control algorithm used by TCP. Present a note on each component. (8) [CO3,K2]

(OR)

b. i) State the significance of flow control service of TCP protocol. Explain how it eliminates the possibility of the sender overflowing the receiver's buffer. (8) [CO3,K2]

ii) With a neat sketch, illustrate how TCP connection is established and closed between two hosts. (8) [CO3,K2]

14. a. i) Write the steps in LS routing algorithm. Apply the same and find the shortest path between A and all the nodes in the following graph (10) [CO4,K3]

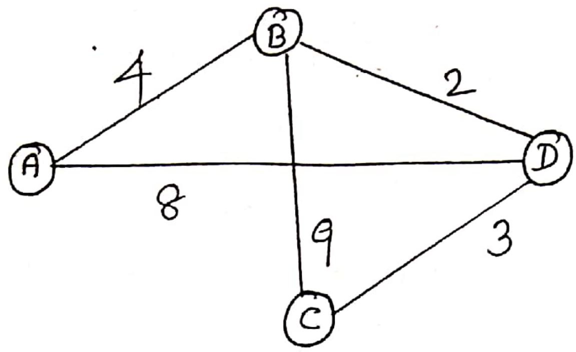


ii) List the components of SDN controller, and highlight the role of each component. (6). [CO4,K2]

(OR)

b. i) Name the packet scheduling algorithms. Explain any two of them. (6) [CO4,K2]

ii) Write the distance vector routing algorithm. Apply the same and find the routing table at all the routers (A, B, C and D) in the following graph. (10) [CO4,K3]



15. a. i) List the operations of a slotted ALOHA protocol. (5) [CO5,K1]

ii) Identify different types of error detection and correction mechanisms supported at the link layer. With examples, illustrate any two of them (11) [CO5,K2]

(OR)

b. i) Enumerate the steps in CSMA/CD from the perspective of adapter attached to a broadcast channel. (5) [CO5,K1]

ii) Summarize the different symmetric key cryptography algorithms. Provide suitable examples. (11) [CO5,K2]

Bloom's Taxonomy Level	Remembering (K1)	Understanding (K2)	Applying (K3)	Analysing (K4)	Evaluating (K5)	Creating (K6)
Percentage	21	47	32	-	-	-

KONGU ENGINEERING COLLEGE, PERUNDURAI, ERODE – 638 060

Semester Examination – December 2022

Programme : BE
Branch : CSE Semester : V   Course : 20CST51 – Computer Networks

Answer Key
PART A (10 x 2 = 20 Marks)

1. **Processing Delay**
- Time required for every intermediate node and the source to process the message in order to move it to the intended destination
- Processing delay is in the order of microseconds or less

Queuing Delay
- The amount of time spent by a packet at the router queue is called as Queuing delay
- Queuing delay is in the order of microseconds to milliseconds

2.

Packet Switching	Circuit Switching
Packet switching allocates link on demand	Circuit switching pre-allocates the transmission link regardless of demand from the user
Packet switching is simpler, more efficient and less costly than circuit switching	Circuit switch network is efficient when it is working at its full capacity. But most of the time circuit switching is inefficient because it is working at partial capacity
Packet switching enables the sender to transfer the data to the receiver not at guaranteed constant rate	Circuit switching enables the sender to transfer the data to the receiver at guaranteed constant rate

3. **(any 2 applications 1mark each)**

Internet Applications	Application layer protocol
E-mail	SMTP
Web Documents Access	HTTP
File Transfer	FTP
Remote Terminal Access	Telnet

4. **Handshaking**
- TCP client and server exchange transport layer control information with each other before the application-level messages begin to flow. This so-called handshaking procedure that alerts the client and server allowing them to prepare for a transmission of packets.

5. Given, Datagram size = 3000 bytes
MTU of link = 500 bytes

The maximum size of data field in each fragment = 480 (20 bytes IP header).
Thus the number of required fragments 7
(3000-20)/480 = 7

6. **Significance of Selective Repeat Protocol**

- In Go-Back-N protocol, when a single packet is lost or corrupted sender resends all packets from the lost packet even though some of these packets may be received safely by the receiver. Resending of all packets from the lost packet makes the network congested. To overcome this problem, Selective Repeat protocol is proposed
- **Selective Repeat protocol is used to resend only selected packets that are actually lost**.

7. **Importance of CIDR Addressing**

- In classless addressing, we can have variable prefix length
- In order to find the prefix length (n) in case of classless addressing, a notation called slash notation or classless interdomain routing(CIDR) is used.

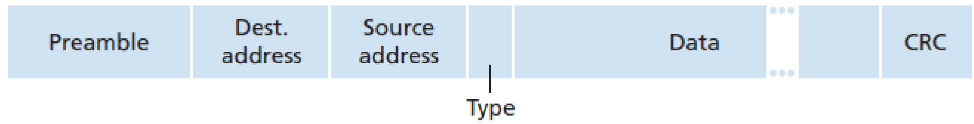
8. **Role of DHCP in network applications**

- DHCP is the protocol used to assign IP address for a newly arrived client system in a network
- In addition to IP address assignment, DHCP also allows a host to learn additional information, such as its subnet mask, the address of its first-hop router and the address of its local DNS server

9. **Purpose of ARP protocol in a network**

- ARP accepts an IP address from the IP protocol, maps it to the corresponding link-layer address (MAC address) and passes it to the data- link layer.

10. **Ethernet Frame Structure**



PART B (5 x 16 = 80 marks)

11. a. i)

1. Propagation Delay (1 mark)

Propagation Delay, d_{prop} = **Distance / Speed = m/s**

2. Transmission Time (1 mark)

Transmission Time, d_{trans} = **Message Size / Transmission Rate = L/R**

3. End-to-End Delay (1 mark)

End-to-End Delay, $d_{end\text{-}to\text{-}end} = \mathbf{d_{prop} + d_{trans} = (m/s) + (L/R)}$

4. (2 marks)

At time $t = d_{trans}$, the last bit of the packet would have reached the start of the transmission medium, and be ready to be transmitted to the receiver.

5. Find the distance 'm' (3 marks)

Given $s = 2.5 * 10^8$ m/s

$L = 1000$ bytes

$R = 10$ Mbps

d_{trans} = Message Size / Transmission Rate = L/R

= 2000 bytes / (10 Mbps)

$= (2000 * 8) / (10 * 10^6)$

$d_{trans} = 16 * 10^{-4}$ seconds

Since given $d_{trans} = d_{prop}$, $d_{prop} = 16 * 10^{-4}$ seconds

d_{prop} = Distance / Speed = m/s

$16 * 10^{-4} = m/(2.5 * 10^8)$

m = 4,00,000 meters = 400 km

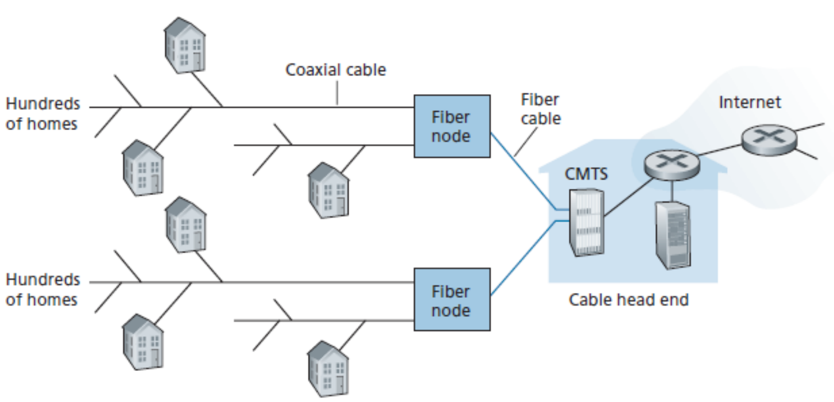
11.a. ii)

Different Types of Access Networks

(2 marks to each)

1. Access networks: Cable-based access

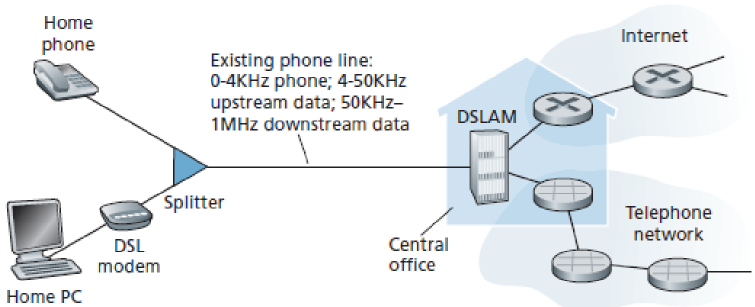
- Cable Internet access makes use of the cable television company's existing cable television infrastructure
- Cable internet access requires special modems, called cable modems



2. Access networks: Digital Subscriber Line (DSL)

Residence obtains DSL Internet access from the same local telephone company

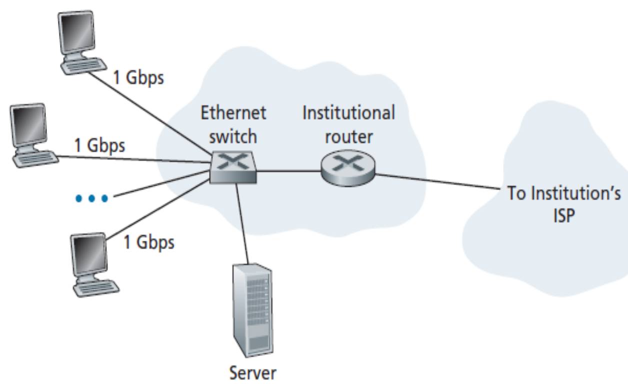
- The DSL standards define multiple transmission rates, including downstream transmission rates of 24 Mbs and 52 Mbs, and upstream rates of 3.5 Mbps and 16 Mbps
- uses existing local telephone infrastructure



<u>3. Access networks: Enterprise networks</u>

<u>Ethernet</u>

- Ethernet is the prevalent access technology in corporate, university, and home networks
- With Ethernet access, users typically have 100 Mbps to tens of Gbps access to the Ethernet switch



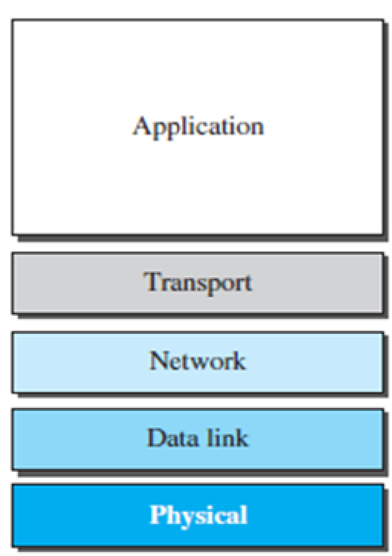
<u>WiFi</u>

- People are accessing the Internet wirelessly from laptops, smartphones, tablets and others
- In a wireless LAN setting, wireless users transmit/receive packets to/from an access point that is connected into the enterprise's network
- Wireless LAN access based on IEEE 802.11 technology known as WiFi

11. b. i)

<u>IP Protocol Stack</u>

<u>Diagram</u> **(3 marks)**



TCP/IP Protocol Suite

(Explanation of each layer 5 marks)

Application Layer

- This layer is used to allow access to network resources
- Protocols used in this layer are WWW, HTTP, FTP, DNS, SMTP, SSH etc. These protocols are used for network services like Web surfing, File transfer, Emails etc.

Transport Layer

- Transport layer is responsible for process-to-process delivery, Flow control, Error control, Congestion control, connection-oriented and connectionless services
- Protocols used in this layer TCP, UDP

Network Layer

- Network layer is responsible for logical addressing, Routing and path determination
- Protocols used in this layer are IP, ICMP

Data Link Layer

- Data Link layer is responsible for framing, Error control, Flow control, Media access control
- Protocol used in this layer are ARP, CSMA, ALOHA, Ethernet

Physical Layer

- Duty of the physical layer to convert data in bits to signals in order to be transmitted through the transmission medium

11.b. ii)

Given, Distance, m = 20,000kms

R = 5Mbps

Speed = $2.5 * 10^8$

1. Bandwidth-Delay product (4 marks)

$$d_{prop} = \text{Distance / Speed}$$
$$= (20000 * 10^3) / (2.5 * 10^8)$$
$$\mathbf{= 0.08\ seconds}$$

$$\text{Bandwidth-Delay product} = R * d_{prop}$$
$$= (5 * 10^6) * (0.08)$$
$$\mathbf{= 0.4 * 10^6\ bits = 4 * 10^5\ bits}$$

2. Maximum number of bits that will be in the link at any given time (2 marks)

Maximum number of bits in the link = $\min(4 * 10^5, 8*10^5) = 4 * 10^5$ bits

3. Width of a bit in the link (2 marks)

Width of a bit = length of link/bandwidth-delay

$$\text{Width of a bit} = m/(R \cdot d_{prop})$$
$$= (20{,}000 * 10^3) / (4 * 10^5)$$
$$= 50$$

12. a. i)

TCP Program for Server (Using any one of the languages C/C++/Java/Python) - 10 marks

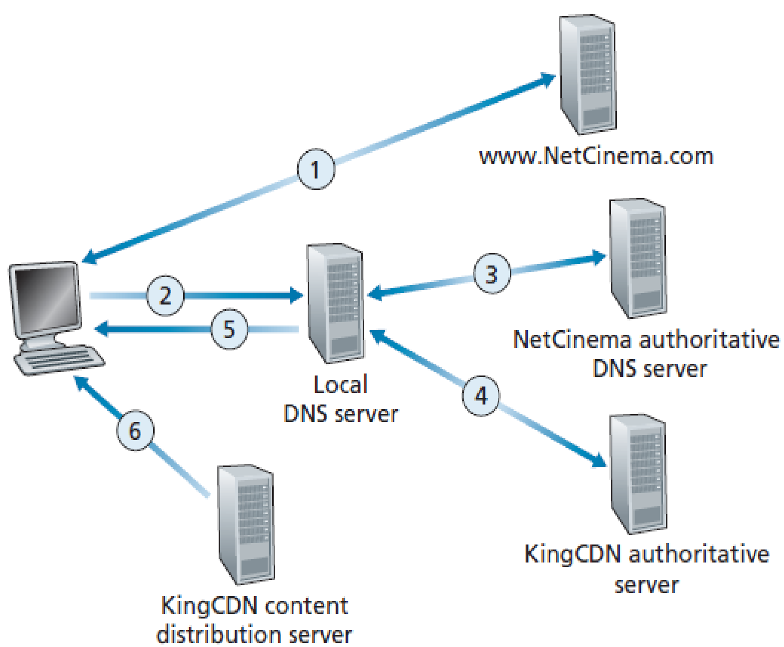
```
import java.net.*;
import java.io.*;

public class Server
{
       public static void main(String args[])
      {
            ServerSocket   server = new ServerSocket(5000);
            System.out.println("Server started");
            System.out.println("Waiting for a client ...");
            Socket          socket    = server.accept();
            System.out.println("Client accepted");
```

```
            DataInputStream   in = new DataInputStream(new  BufferedInputStream
                                                    (socket.getInputStream()));

            String line = "";
            // reads message from client until "Over" is sent
            while (!line.equals("Over"))
            {
                line = in.readUTF();
                System.out.println(line);
            }
            System.out.println("Closing connection");
            socket.close();
        }
    }
```

12.a. ii)

Steps involved when DNS server redirects user request to a CDN server

Diagram (4 marks)



Steps (2 marks)

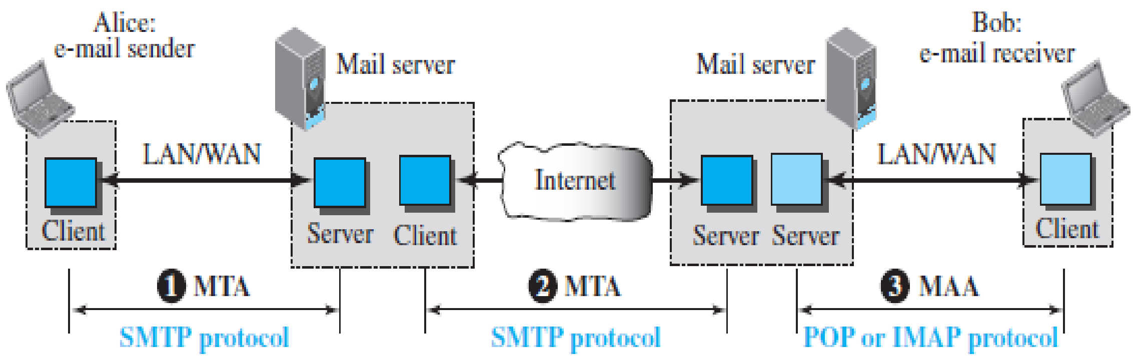
1. The user visits the Web page at NetCinema
2. When the user clicks on the link http://video.netcinema.com/6Y7B23V, the user's sends a DNS query for video.netcinema.com.
3. The user's Local DNS Server (LDNS) relays the DNS query to an authoritative DNS server which observes the string "video" in the hostname video.netcinema.com. To "hand over" the DNS query to KingCDN, instead of returning an IP address, the NetCinema authoritative DNS server returns to the LDNS a hostname in the KingCDN's domain
4. The user's LDNS then sends a second query, and KingCDN's DNS system eventually returns the IP addresses of a KingCDN
5. The LDNS forwards the IP address of the content-serving CDN node to the user's host.
6. Once the client receives the IP address for a KingCDN content server, it issues an HTTP GET request for the video.

12. b.i)

E-mail

- The following are the application layer protocols that are used to move message from source to destination **(2marks)**
    1. SMTP
    2. POP or IMAP protocols

Diagram (4 marks)



Message Transfer Agent: SMTP **(2 marks)**

- SMTP (Simple Mail Transfer Protocol) uses commands and responses to transfer messages between MTA client and MTA server
- SMTP protocol is used for communication from client to mail server at its side and for communication between two mail servers

POP3 and IMAP4 **(2marks)**

- POP3: Post Office Protocol, version 3
- IMAP4: Internet Mail Access Protocol, version 4
- POP3 and IMAP4 are called as mail access protocols used at receiver side

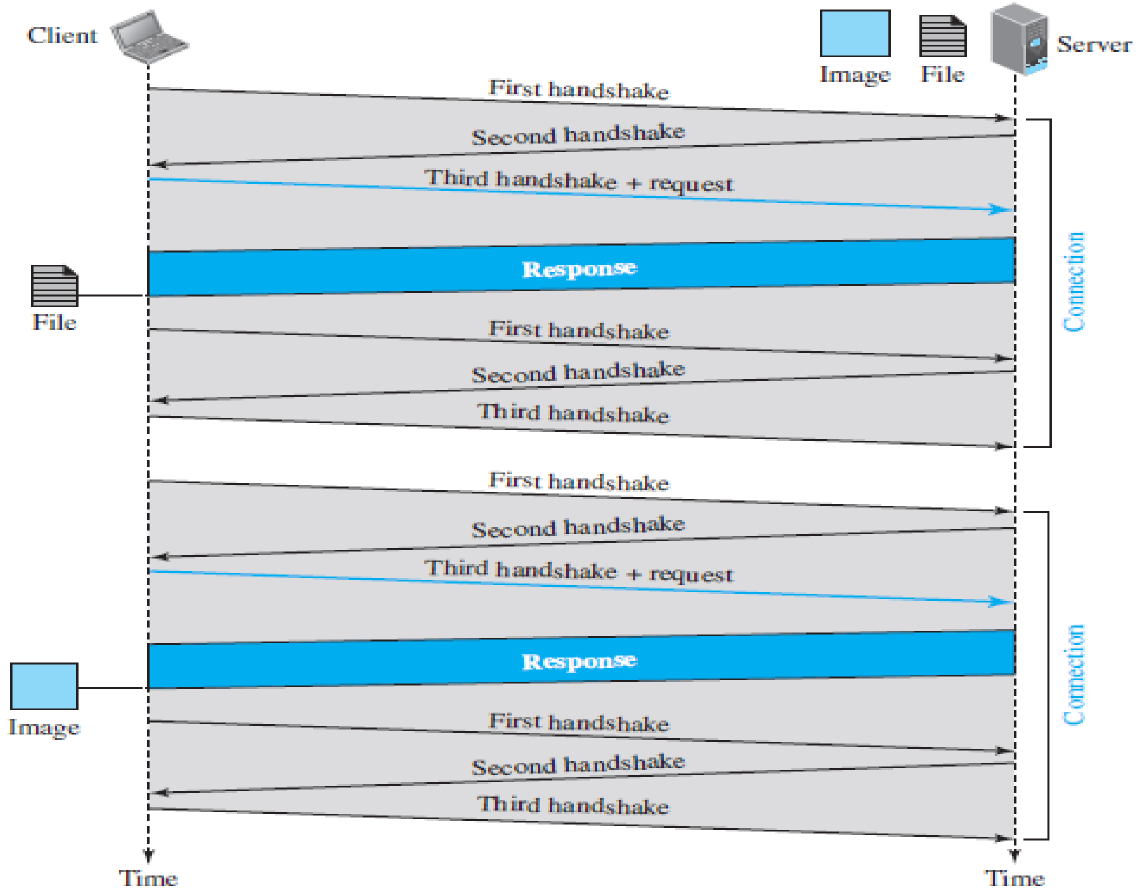
12. b.ii)

Transferring a web page from server to client using Non-persistent connections

Non-persistent Connection **(2 marks)**

- One TCP connection is created for each request/response
- Imposes big overhead

Steps in transferring a web page from server to client

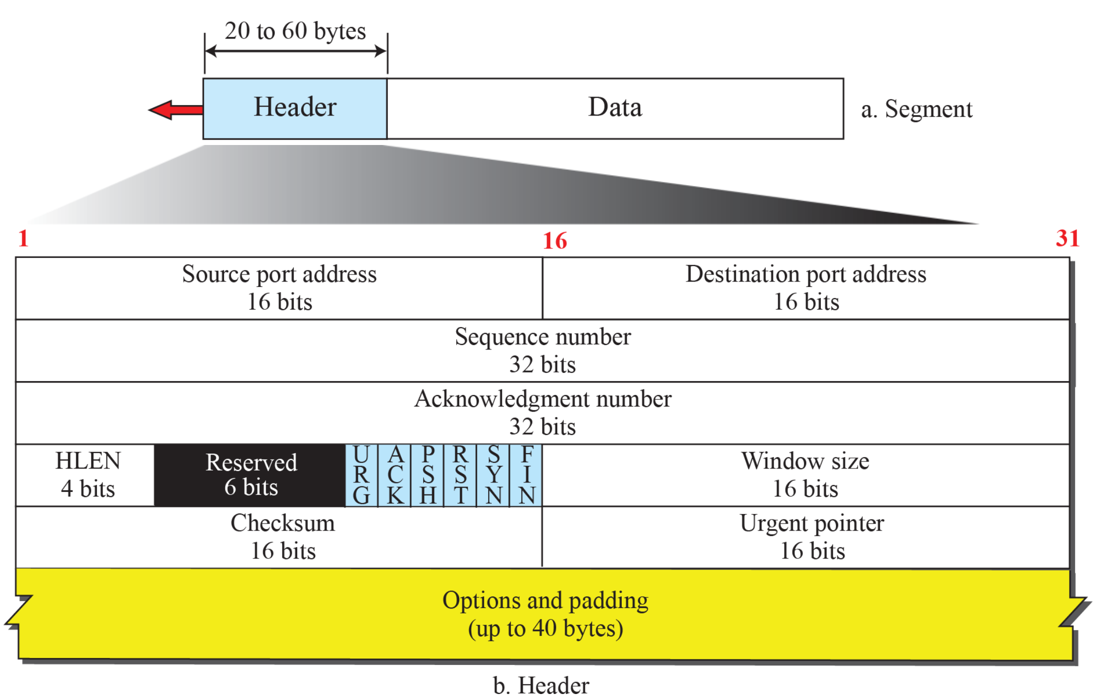


(Diagram + Explanation 4 marks)

13. a.i)

<u>Structure of TCP Header</u>

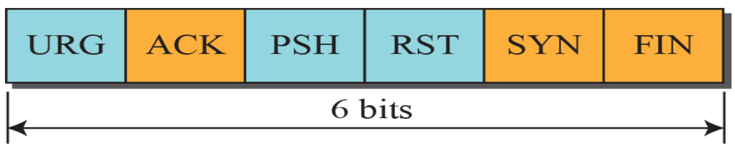
(Diagram 4 marks)



(Explanation of fields 4 marks)

Various fields in the TCP header are as follows:

1. <u>Source port number (16 bits):</u> This field defines the port number of process running at source side
2. <u>Destination port number (16 bits):</u> This field defines the port number of process running at destination side
3. <u>Sequence number (32 bits):</u> This field defines the number assigned to each segment
4. <u>Acknowledgment number (32 bits):</u> This field defines the number assigned to acknowledgment segment
5. <u>Header length (4 bits):</u> This field contains the length of header. The value in this field should be multiplied by 4 to get actual header length
6. <u>Control field/ flag field (6 bits):</u> The 6 bits control field says what type of segment it is.



7. <u>Window size (16 bits):</u> This field is used to announce the window size of each side to the other side. This window size is also called as receive window size
8. <u>Checksum (16 bits):</u> This field is used for error detection
9. <u>Urgent Pointer (16 bits):</u> This field is used when URG(Urgent bit) bit is set in the control field. The field contains the byte number where the urgent data ends in the data field
10. <u>Options (0 to 40 bytes):</u> This field can be used to include some extra information if needed

13. a.ii)

<u>Congestion Control Algorithm by TCP</u>

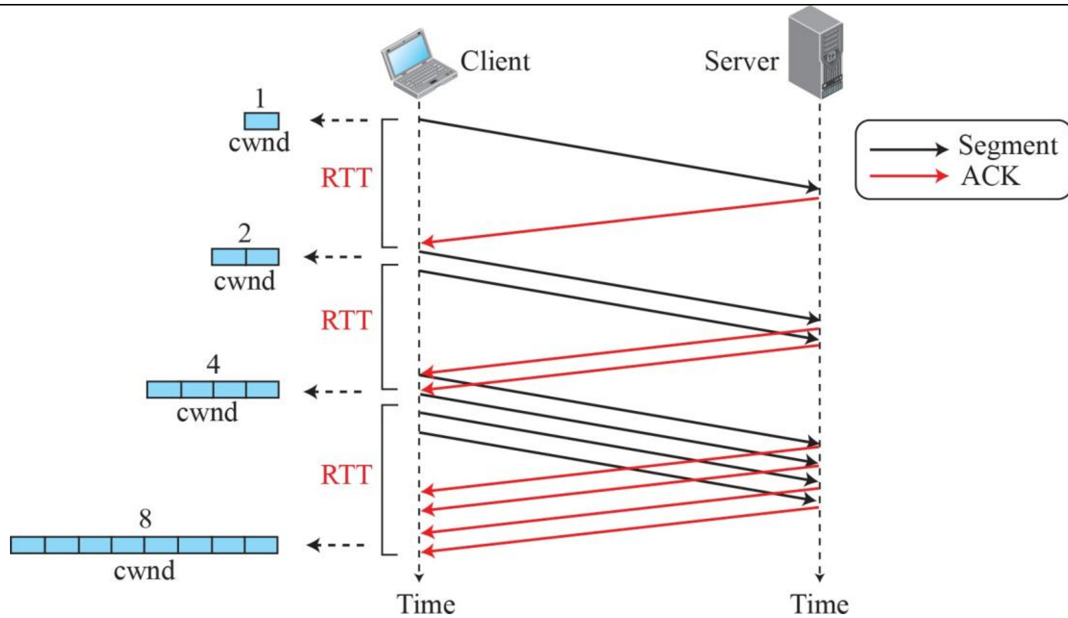
- Handling congestion is based on three algorithms: **(2 marks)**
  1. Slow start: Exponential Increase
  2. Congestion avoidance: Additive increase
  3. Fast Recovery

1. <u>Slow start: Exponential Increase</u> (2marks)

- If an ACK arrives cwnd=cwnd+1

$$\text{Start} \rightarrow cwnd = 1 \rightarrow 2^0$$
$$cwnd = cwnd + 1 = 1 + 1 = 2 \rightarrow 2^1$$
$$cwnd = cwnd + 2 = 2 + 2 = 4 \rightarrow 2^2$$
$$cwnd = cwnd + 4 = 4 + 4 = 8 \rightarrow 2^3$$

- In slow-start the size of congestion window increases exponentially until it reaches a threshold value called ssthresh (slow start threshold value)
- When it reaches threshold value slow start stops and next phase starts



2. Congestion avoidance, Additive Increase (2 marks)

- If an ACK arrives cwnd = cwnd+(1/cwnd)

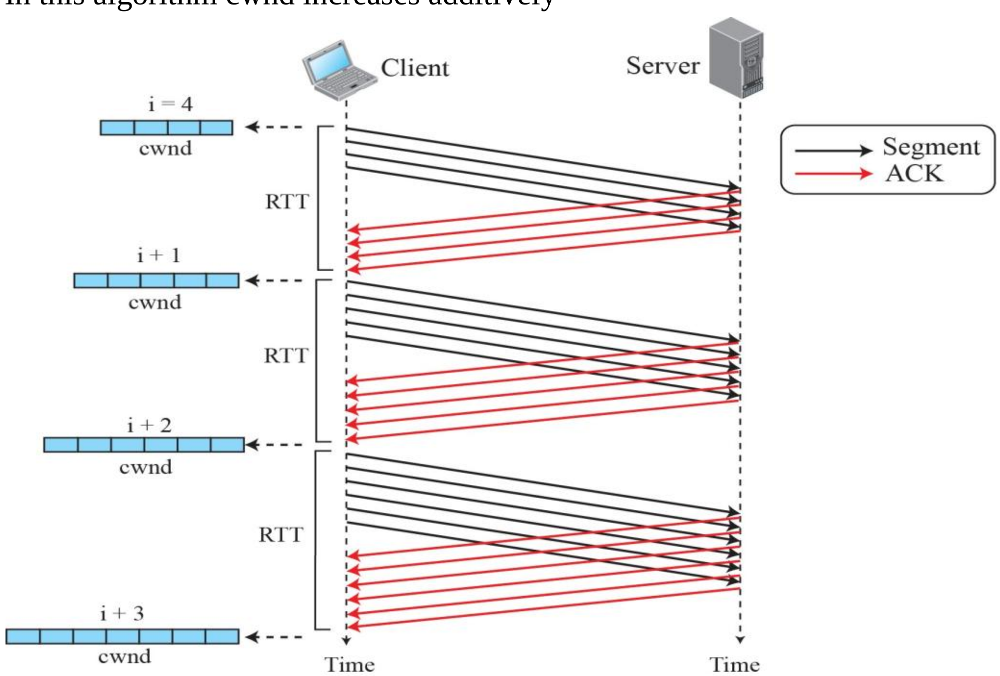
Start → cwnd = i

cwnd = i + 1

cwnd = i + 2

cwnd = i + 3

- In this algorithm cwnd increases additively



3. Fast Recovery (2 marks)

- This fast recovery policy is used when 3 duplicate ACKs received.
- Here cwnd is increased in exponential manner only when duplicate ACK is received
- If an duplicate ACK arrives cwnd=cwnd+1
- Used in new version of TCP

13.b. i)

<u>Flow Control service of TCP protocol</u>

<u>Significance of Flow Control</u> (2 marks)

- TCP provides a flow-control service to its applications to eliminate sender overflowing the receiver's buffer.
- Flow control is called as speed matching service: matching the rate at which the sender is sending against the rate at which the receiving application is reading.
- TCP provides flow control by maintaining a variable called the receive window
- At receiver side a buffer is maintained for holding packets called as Receive Buffer. How much free space is available at receive buffer is indicated by receive window and this receive window value is given to sender using the field window size in TCP header

Diagram(3 marks)

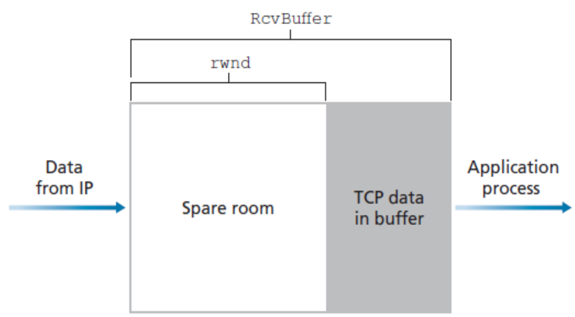


Figure 3.38 ♦ The receive window (rwnd) and the receive buffer (RcvBuffer)

Explanation (3 marks)

- Once sender gets the receive window size (free space in receive buffer), sender sets its send window size
- By setting send window size that equals to receive window, TCP is ensuring, sender is not going to overflow the receive buffer thereby providing flow control service
- At receiver side in order to ensure not to overflow the allocated buffer, we must have

$$\text{LastByteRcvd} - \text{LastByteRead} <= \text{RcvBuffer}$$

- The size of receive window is calculated as,

$$\text{rwnd} = \text{RcvBuffer} - [\text{LastByteRcvd} - \text{LastByteRead}]$$

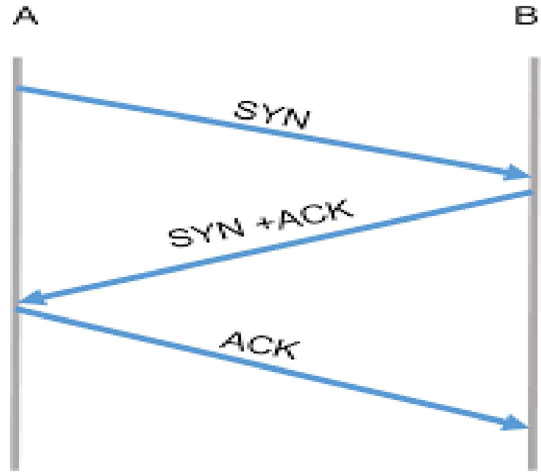
- At sender side the number of bytes sent should follow the below formula in order to ensure flow control

$$\text{LastByteSent} - \text{LastByteAcked} <= \text{rwnd}$$

13. b.ii)

<u>TCP Connection Establishment</u> (Diagram 2 marks + Explanation 2 marks = 4 marks)

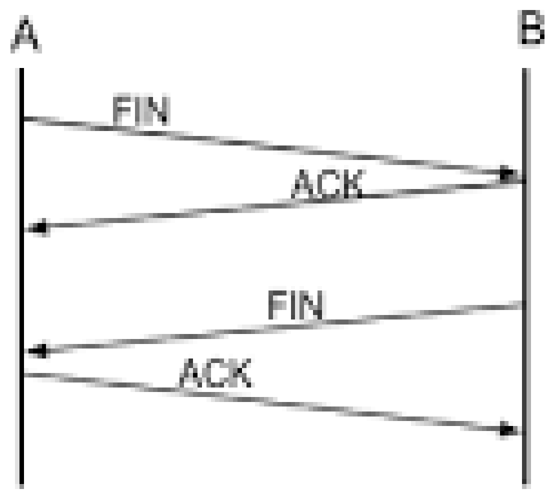
- Connection establishment in TCP is done using three-way handshaking
- During connection establishment SYN (Synchronize) segment is send from sender to receiver. Receiver gives ACK for this SYN plus it also sends the SYN to sender. Sender gives ACK finally. In these three segments except last segment(ACK) remaining segments carries no data



Three way handshake

Connection Termination **((Diagram 2 marks + Explanation 2 marks = 4 marks)**

- During connection termination FIN (Finish) segment is send from sender to receiver. Receiver gives ACK for this FIN plus it also sends the FIN to sender. Sender gives ACK finally. (3-way handshake)
- Connection Termination can be done in Four-way handshaking also where server gives ACK only and after sometimes it gives FIN to client. Finally client gives ACK



14.a. i)

<u>LS routing Algorithm</u> (4 marks)

Dijkstra's link-state routing algorithm

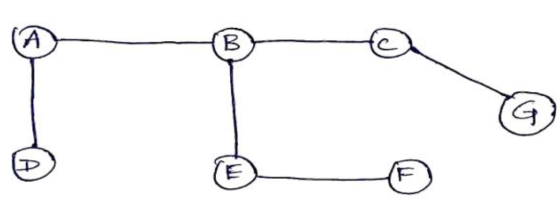
```
Initialization:
  N' = {u}                        /* compute least cost path from u to all other nodes */
  for all nodes v
    if v adjacent to u            /* u initially knows direct-path-cost only to direct neighbors */
      then D(v) = c_u,v           /* but may not be minimum cost! */
    else D(v) = ∞

Loop
   find w not in N' such that D(w) is a minimum
   add w to N'
   update D(v) for all v adjacent to w and not in N' :
      D(v) = min ( D(v), D(w) + c_w,v )
   /* new least-path-cost to v is either old least-cost-path to v or known
   least-cost-path to w plus direct-cost from w to v */
until all nodes in N'
```

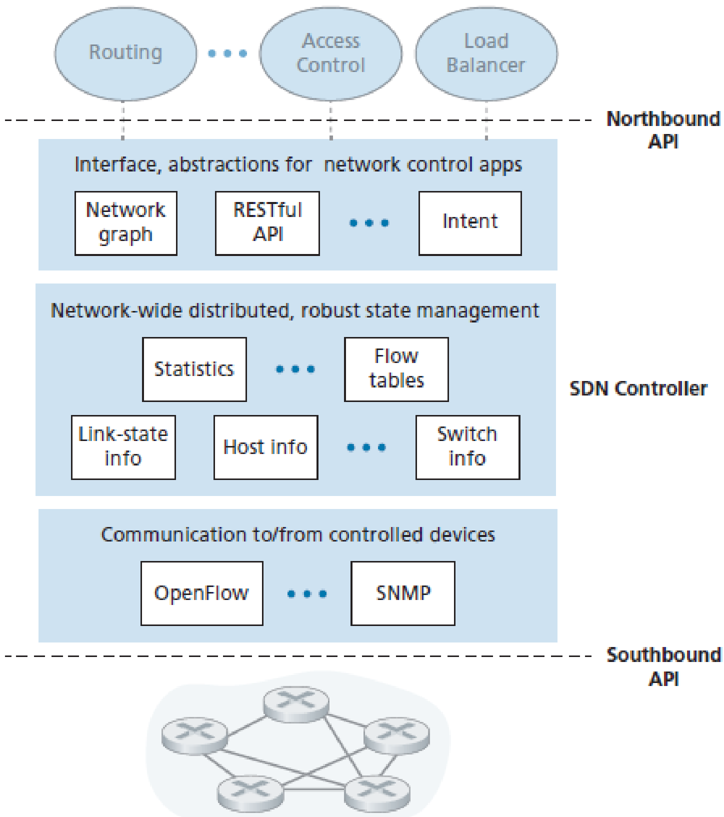
<u>Shortest path between A to all the nodes</u> (5 marks)

N'	B	C	D	E	F	G
A	2,A	∞	3,A	∞	∞	∞
AB		7,B	3,A	4,B	∞	∞
ABD		7,B		4,B	∞	∞
ABDE		7,B			7,E	∞
ABDEC					7,E	9,C
ABDECF						9,C
ABDECFG						

(1 mark)

Least Cost path at A (shortest path)



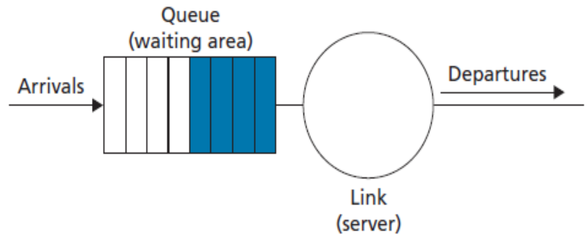
14.a. ii)	<u>**Components of SDN controller**</u> **(2 marks)** 1. A communication layer: communicating between the SDN controller and controlled network devices 2. A network-wide state-management layer 3. The interface to the network-control application layer <u>**Diagram (2 marks)**</u>  **(Explanation 2 marks)** 1. <u>A communication layer: communicating between the SDN controller and controlled network devices</u> • a protocol is needed to transfer information between the controller and the device • constitutes the lowest layer of the controller architecture • The communication between the controller and the controlled devices has come to be known as the controller's "southbound" interface 2. <u>A network-wide state-management layer</u> • the controller have upto-date information about state of the networks' hosts, links, switches, and other SDN-controlled devices • a controller might also maintain a copy of flow tables for the various controlled devices 3. <u>The interface to the network-control application layer</u> • The controller interacts with network-control applications through its "northbound" interface • This API allows network-control applications to read/write network state and flow tables within the state-management layer
14.b. i)	<u>**Packet Scheduling Algorithms**</u> **(2 mark)** • When packets are queued at the router, the following scheduling mechanisms are used for determining the order in which queued packets are transmitted over an outgoing link

1. First-in-First-Out (FIFO)
2. Priority Queuing
3. Round Robin
4. Weighted Fair Queuing (WFQ)

(Explanation of any 2 with 2 marks each)

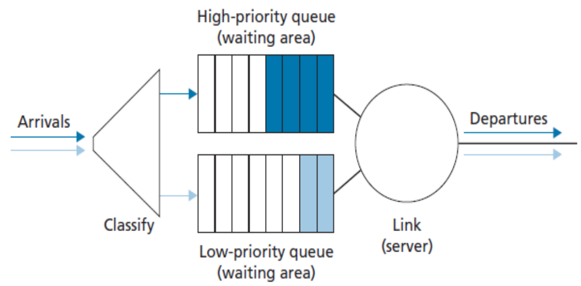
1. First-in-First-Out (FIFO)

- The FIFO scheduling discipline selects packets for link transmission in the same order in which they arrived at the output link queue.



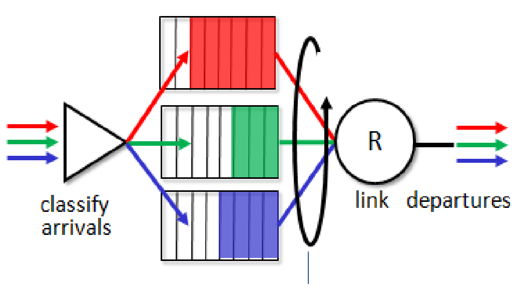
2. Priority Queuing

- In priority queuing, packets arriving at the output link are classified into priority classes
- Each priority class typically has its own queue
- After completing high priority queue control will to low priority queue



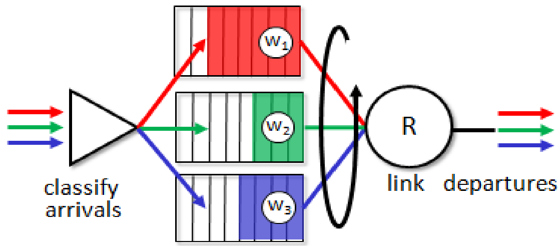
3. Round Robin scheduling

- Under the round robin queuing discipline, packets are sorted into classes as with priority queuing. However, rather than there being a strict service priority among classes, a round robin scheduler alternates service among the classes.



4. Weighted Fair Queuing (WFQ) scheduling

- As in round robin scheduling, a WFQ scheduler will serve classes in a circular manner
- In WFQ scheduling each class, i, is assigned a weight w_i



14. b.ii) **Distance Vector Routing Algorithm** **(4 marks)**

Table 20.1 *Distance-Vector Routing Algorithm for a Node*

```
Distance_Vector_Routing ( )
{
    // Initialize (create initial vectors for the node)
    D[myself] = 0
```

Table 20.1 *Distance-Vector Routing Algorithm for a Node (continued)*

```
    for (y = 1 to N)
    {
        if (y is a neighbor)
            D[y] = c[myself][y]
        else
            D[y] = ∞
    }
    send vector {D[1], D[2], …, D[N]} to all neighbors
    // Update (improve the vector with the vector received from a neighbor)
    repeat (forever)
    {
        wait (for a vector Dw from a neighbor w or any change in the link)
        for (y = 1 to N)
        {
            D[y] = min [D[y], (c[myself][w] + Dw[y ])]      // Bellman-Ford equation
        }
        if (any change in the vector)
            send vector {D[1], D[2], …, D[N]} to all neighbors
    }
} // End of Distance Vector
```

Routing Table at routers(A, B, C and D) (5 marks)

Step1:

Initial Distance Vector at A

A	0
B	4
C	∞
D	8

Step2:

	A	Initial DV at B	⇒ Revised A1
A	0	4	0
B	4	0	4
C	∞	9	13
D	8	2	6

Step3:

	A1	Initial DV at D	⇒ Revised A2
A	0	8	0
B	4	2	4
C	13	3	11
D	6	0	6

Step 4:

	A2	Revised B	⇒ Revised A3
A	0	4	0
B	4	0	4
C	11	5	9
D	6	2	6

Step5:

	A3	Revised D	⇒ Revised A4.
A	0	6	0
B	4	2	4
C	9	3	9
D	6	0	6

(1 mark)

> Like above steps, Routing tables for routers B, C, D has been constructed.

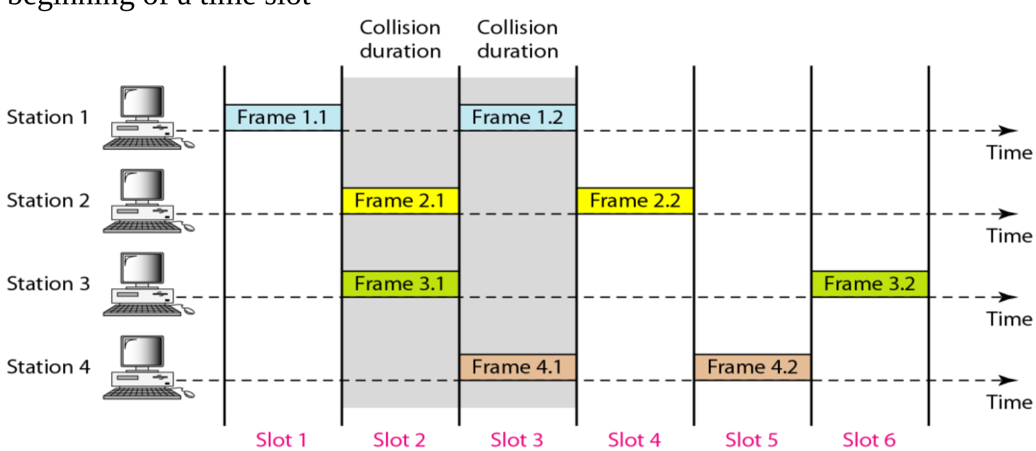
	A	B	C	D
A	0	4	9	6
B	4	0	5	2
C	9	5	0	3
D	6	2	3	0

15. a.i)

<u>Operations of Slotted ALOHA protocol</u>

(Diagram 2.5 marks and Explanation 2.5 marks = 5 marks)

- Slotted ALOHA is used to improve the efficiency of pure ALOHA
- In slotted ALOHA, time is divided into multiple slots and each station sends data only at the beginning of the time slot. A station can't send frames during the middle of a time slot which reduces collision
- Since station sends data only at the beginning of the time slot, collision problem seen in pure ALOHA is reduced here but still collision problem exist when multiple stations send data at the beginning of a time slot



15. a.ii)

<u>Different types of Error Detection and Correction mechanisms</u>

(1 mark)

- 3 types of Error detection and correction techniques are been used:
  1. Parity Check
  2. Cyclic Redundancy Check(CRC)
  3. Checksum

(any two methods with example with 5 marks each)

<u>1.Parity Check</u>

<u>(i) Single Bit Parity Check</u>

- In single bit parity check only one bit is used as Parity bit
- Parity Check can be either Even Parity or Odd Parity
- Single bit Parity check detect only single bit error

<u>Example:</u>

Consider the data =1011. What is the even parity bit at sender side and how it is verified at receiver side

Solution: Data = 1011, Number of 1's in the data is odd. So parity bit =1

ii) Two Dimensional Parity Check

- In two dimensional parity check, data is divided into rows and columns and the parity bits are calculated for each row and column. This method is used for both error detection and correction (specify which bit is corrupted)

Example:

Consider the data unit to be transmitted is

10011001111000100010010010000100

Calculate the parity bits at the sender side if two-dimensional even parity check is used (use 8 bit words)

Solution: Divide data into 8 bits words and put each 8 bits in a row

									Parity Bit for Row
	1	0	0	1	1	0	0	1	0
	1	1	1	0	0	0	1	0	0
	0	0	1	0	0	1	0	0	0
	1	0	0	0	0	1	0	0	0
Parity Bit for column	1	1	0	1	1	0	1	1	0

2. Cyclic Redundancy Check(CRC)

In CRC error Detection method, CRC is calculated using following steps:

1. Initially data is augmented with (divisor-1) zero bits. After that
2. Perform XOR between data and divisor
3. Final remainder is going to be the CRC bits
4. Number of CRC bits is equal to (divisor-1) bits
5. Send data+CRC to receiver
6. At receiver side data+CRC is XOR'ed with divisor
7. If remainder ->zero means No Error

   remainder->non-zero means Error

Example (any one)

3. Checksum

In Checksum error Detection method, checksum is calculated using following steps:

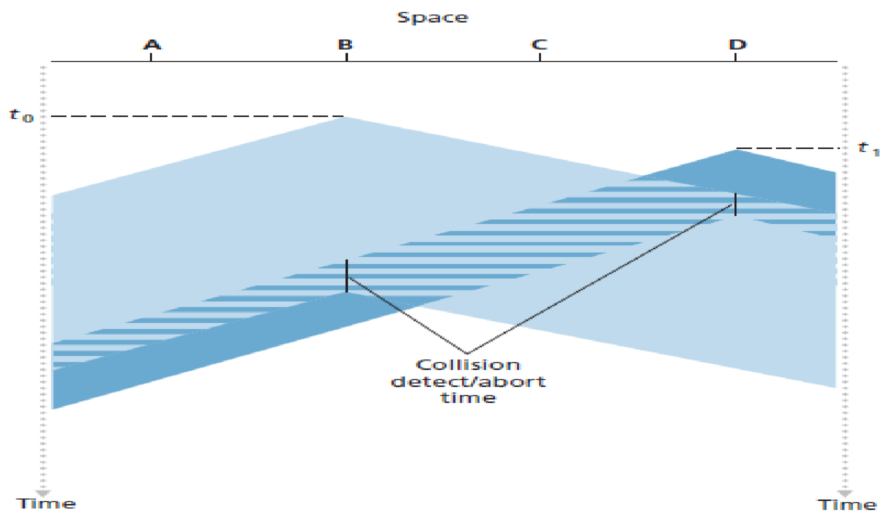
1. Data is divided into 16 bits words(by default data is divided into 16 bits words)
2. Binary addition is performed between each 16 words
3. Calculate the final sum for the given data
4. Take 1's complement for the final sum. This 1's complement result is going to be the checksum
5. Sender sends data + checksum to receiver
6. Receiver do the same steps as like that of sender
7. If final result is Zero -> No Error

   Non zero -> Error

Example (any one)

15. b.i) **Steps in CSMA/CD**

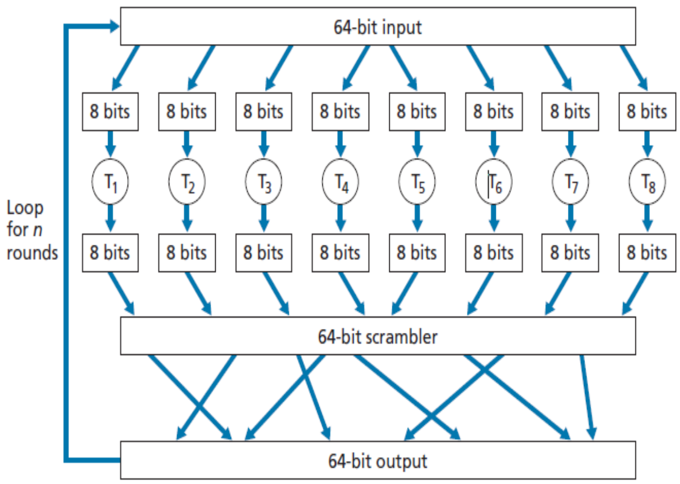
Diagram **(2 marks)**

	 **<u>Steps</u> (3 marks)** 1. The adapter obtains a datagram from the network layer, prepares a link-layer frame, and puts the frame adapter buffer. 2. If the adapter senses that the channel is idle, it starts to transmit the frame. If, on the other hand, the adapter senses that the channel is busy, it waits until it idle and then starts to transmit the frame. 3. While transmitting, the adapter monitors for the presence of signal energy coming from other adapters using the broadcast channel 4. If the adapter transmits the entire frame without detecting signal energy from other adapters, the adapter is finished with the frame. If, on the other hand, the adapter detects signal energy from other adapters while transmitting, it aborts the transmission 5. After aborting, the adapter waits a random amount of time and then returns to step 2
15.b. ii)	**<u>Different symmetric key cryptography algorithms</u>** **<u>Algorithms</u> (1 mark)** 1. Caesar cipher 2. Monoalphabetic cipher 3. Polyalphabetic encryption 4.Block Ciphers **(Explanation each one with example 2.5 marks each = 10 marks)** **1. Caesar cipher** • In Caesar cipher, each letter in the plaintext message is substituted with the letter that is k letters later in the alphabet • <u>Example</u> k = 3, then the letter a in plaintext becomes d in ciphertext; b in plaintext becomes e in ciphertext, and so on **2. Monoalphabetic cipher** • substitutes one letter of the alphabet with another letter of the alphabet • any letter can be substituted for any other letter • <u>Example</u> Plaintext letter: a b c d e f g h i j k l m n o p q r s t u v w x y z Ciphertext letter: m n b v c x z a s d f g h j k l p o i u y t r e w q “hello” becomes “acggk” **3. Polyalphabetic encryption** • polyalphabetic encryption uses multiple monoalphabetic ciphers

- same letter in different positions in the plaintext message encoded differently
- Example
  Plaintext letter: a b c d e f g h i j k l m n o p q r s t u v w x y z
  C1(k = 5): f g h i j k l m n o p q r s t u v w x y z a b c d e
  C2(k = 19): t u v w x y z a b c d e f g h i j k l m n o p q r s
  We choose to use these two Caesar ciphers, C1 and C2, in the repeating pattern C1, C2, C2, C1, C2. The first letter of plaintext is to be encoded using C1, the second and third using C2, the fourth using C1, and the fifth using C

4.Block Ciphers

- used in many secure Internet protocols, including PGP, TLS and IPsec
- In a block cipher, the message to be encrypted is processed in blocks of k bits



Cipher-Block Chaining

- In order to overcome from some difficulties in Block ciphers, Cipher-block chaining has been proposed which introduces some randomness into the ciphertext so that identical plaintext blocks produce different ciphertext blocks.