

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY, RAMAPURAM
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

ANSWER KEY SUBMISSION

Date of Exam & Session	03/05/2023 AN	Category of Exam	CLA3
Course Name	Computer Communications	Course Code	18CSS202J
Name of the Faculty submitting	Dr. M.Ayyadurai	Date of submission of Answer Key	04/05/2023
Department to which the Faculty belongs to	CSE	Total Marks	50

PART A (10 x 1 = 5)
ANSWER ALL THE QUESTIONS

Q.No	Questions	Marks
1	If Data → 011100011110 and End Delimeter → 01111 then, find data after bit stuffing ? a) 01110000111111 b) 01110000111010 c) 01110111111010 d) 01110000111011	1
2	Which one is not the Characteristic of Stop and Wait ARQ? a) Full duplex link b) Closed Loop OR connection oriented c) special category of SWP where its window size is 1 d) special category of SWP where its window size is 1	1
3	Find the hamming distance between the two strings 1101 1001 and 1001 1101. a)3 b)4 c)2 d) 5	1
4	The bit pattern of the flag in HDLC is a)01010101 b)10001000 c)01111110 d)10000001	1
5	_____ Control is the bit-oriented protocol, on the other hand, _____ is the byte-oriented protocol a)PPP,HDLC b)HDLC,PPP c)ICMP,AODV d)HDLC,AODV	1
6	In OSPF header, which field is used to detect errors in the packet? a) Type b) Area ID c) Authentication type d) Checksum	1
7	Administrative distance for internal EIGRP is _____ a) 90 b) 170 c) 110 d) 91	1
8	EIGRP uses the _____ algorithm for finding shortest path. a) SPF b) DUAL c) Linkstate d) Dijkstraalgo	1

9	Which command displays RIP routing updates? a) Show IP route b) Debug IP RIP c) Show protocols d) Debug IP route	1
10	Which protocol should you select if the network diameter is more than 17 hops? a) RIPv1 b) RIPv2 c) EIGRP d) All of the above	1

PART B (4x4= 16)

ANSWER ANY FOUR QUESTIONS

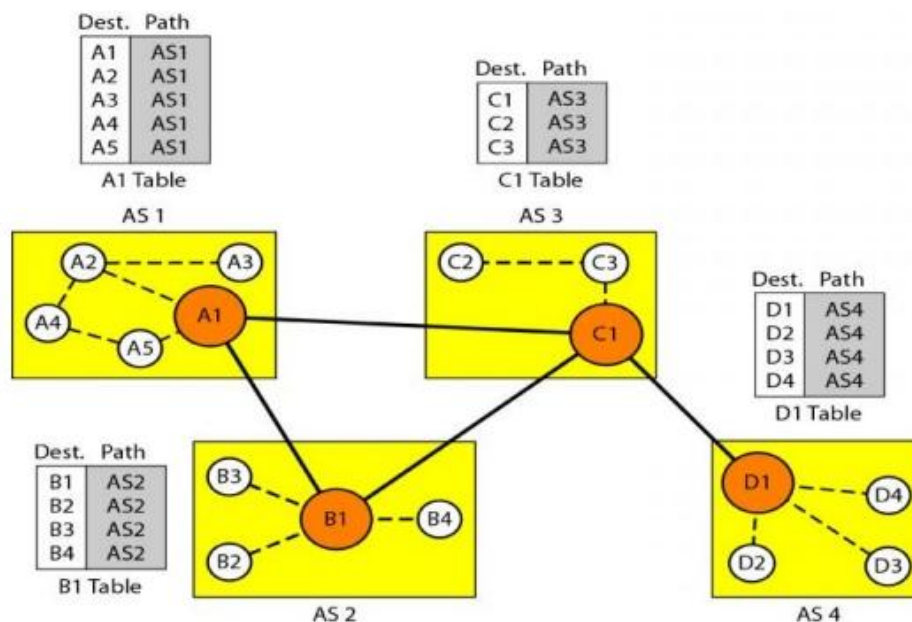
Q.No	Questions	Marks
11.	<p>Analyze the working of Stop and Wait ARQ with diagram</p> <p style="text-align: right;">(2)</p> <ol style="list-style-type: none"> 1) Sender A sends a data frame or packet with sequence number 0. 2) Receiver B, after receiving data frame, sends an acknowledgement with sequence number 1 (sequence number of next expected data frame or packet) <p>There is only one bit sequence number that implies that both sender and receiver have buffer for one frame or packet only.</p> <ul style="list-style-type: none"> • It uses link between sender and receiver as half duplex link • Throughput = 1 Data packet/frame per RTT • If Bandwidth*Delay product is very high, then stop and wait protocol is not so useful. The sender has to keep waiting for acknowledgements before sending the processed next packet. • It is an example for “Closed Loop OR connection oriented “ protocols • It is a special category of SWP where its window size is 1 • Irrespective of number of packets sender is having stop and wait protocol requires only 2 sequence numbers 0 and 1 <p style="text-align: right;">(2)</p>	4
12.	<p>Apply CRC checking method to predict the error with example.</p> <p>Unlike checksum scheme, which is based on addition, CRC is based on binary division.</p> <ol style="list-style-type: none"> 1. In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number. 2. At the destination, the incoming data unit is divided by the same number. If at this 	4

	<p>step there is no remainder, the data unit is assumed to be correct and is therefore accepted.</p> <p>3.A remainder indicates that the data unit has been damaged in transit and therefore must be rejected. (2)</p> <div style="display: flex; justify-content: space-around; align-items: flex-start;"> <div style="text-align: center;"> <p>original message 1 0 1 0 0 0 0</p> <p>@ means X-OR</p> <p>Sender</p> <pre> 1001 1010000000 @1001 ----- 0011 000000 @1001 ----- 01010000 @1001 ----- 0011000 @1001 ----- 01010 @1001 ----- 0011 </pre> <p>Message to be transmitted</p> <pre> 1010000000 + 011 ----- 1010000011 </pre> </div> <div style="text-align: center;"> <p>Generator polynomial x^3+1</p> <p>CRC generator 1 0 0 1 4-bit</p> </div> <div style="border: 1px solid black; padding: 5px; font-size: small;"> <p>If CRC generator is of n bit then append $(n-1)$ zeros in the end of original message</p> </div> </div> <div style="display: flex; justify-content: space-around; align-items: flex-start; margin-top: 20px;"> <div style="text-align: center;"> <pre> 1001 1010000011 @1001 ----- 0011 000011 @1001 ----- 01010011 @1001 ----- 0011011 @1001 ----- 01001 @1001 ----- 0000 </pre> <p>Zero means data is accepted</p> </div> <div style="text-align: center;"> <p>Receiver</p> </div> </div> <p style="text-align: right;">(2)</p>																
13.	<p>Compare four popularly used error correction codes.</p> <p>Hamming Codes – It is a block code that is capable of detecting up to two simultaneous bit errors and correcting single-bit errors. (1)</p> <p>Binary Convolution Code – Here, an encoder processes an input sequence of bits of arbitrary length and generates a sequence of output bits. (1)</p> <p>Reed - Solomon Code – They are block codes that are capable of correcting burst errors in the received data block. (1)</p> <p>Low-Density Parity Check Code – It is a block code specified by a parity-check matrix containing a low density of 1s. They are suitable for large block sizes in very noisy channels. (1)</p>	4															
14	<p>Give the significance of routing table in routing algorithm</p> <p>Routing Table:</p> <p>A routing table is a set of rules, often viewed in table format, that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed. All IP-enabled devices, including routers and switches, use routing tables. See below a Routing Table:</p> <table style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #f2f2f2;"> <th style="text-align: left;">Destination</th><th style="text-align: left;">Subnet mask</th><th style="text-align: left;">Interface</th></tr> </thead> <tbody> <tr> <td>128.75.43.0</td><td>255.255.255.0</td><td>Eth0</td></tr> <tr> <td>128.75.43.0</td><td>255.255.255.128</td><td>Eth1</td></tr> <tr> <td>192.12.17.5</td><td>255.255.255.255</td><td>Eth3</td></tr> <tr> <td>default</td><td></td><td>Eth2</td></tr> </tbody> </table> <p>The entry corresponding to the <i>default</i> gateway configuration is a network destination of 0.0.0.0 with a network mask (netmask) of 0.0.0.0. The Subnet Mask of default route is always 255.255.255.255 .</p>	Destination	Subnet mask	Interface	128.75.43.0	255.255.255.0	Eth0	128.75.43.0	255.255.255.128	Eth1	192.12.17.5	255.255.255.255	Eth3	default		Eth2	4
Destination	Subnet mask	Interface															
128.75.43.0	255.255.255.0	Eth0															
128.75.43.0	255.255.255.128	Eth1															
192.12.17.5	255.255.255.255	Eth3															
default		Eth2															

	<p>Entries of an IP Routing Table:</p> <p>A routing table contains the information necessary to forward a packet along the best path toward its destination. Each packet contains information about its origin and destination. Routing Table provides the device with instructions for sending the packet to the next hop on its route across the network. (2)</p> <p>Each entry in the routing table consists of the following entries:</p> <ol style="list-style-type: none"> Network ID: The network ID or destination corresponding to the route. Subnet Mask: The mask that is used to match a destination IP address to the network ID. Next Hop: The IP address to which the packet is forwarded Outgoing Interface: Outgoing interface the packet should go out to reach the destination network. Metric: A common use of the metric is to indicate the <i>minimum number of hops</i> (routers crossed) to the network ID. (2) 													
15	<p>Compare Intra domain and Inter-domain routing protocol</p> <table border="1"> <thead> <tr> <th>S. NO</th><th>INTRADOMAIN ROUTING</th><th>INTERDOMAIN ROUTING</th></tr> </thead> <tbody> <tr> <td>1.</td><td>Routing algorithm works only within domains.</td><td>Routing algorithm works within and between domains.</td></tr> <tr> <td>2.</td><td>It need to know only about other routers within their domain.</td><td>It need to know only about other routers within and between their domain.</td></tr> <tr> <td>3.</td><td>Protocols used in intradomain routing are known as Interior-gateway protocols.</td><td>Protocols used in interdomain routing are known as Exterior-gateway protocols.</td></tr> </tbody> </table>	S. NO	INTRADOMAIN ROUTING	INTERDOMAIN ROUTING	1.	Routing algorithm works only within domains.	Routing algorithm works within and between domains.	2.	It need to know only about other routers within their domain.	It need to know only about other routers within and between their domain.	3.	Protocols used in intradomain routing are known as Interior-gateway protocols.	Protocols used in interdomain routing are known as Exterior-gateway protocols.	4
S. NO	INTRADOMAIN ROUTING	INTERDOMAIN ROUTING												
1.	Routing algorithm works only within domains.	Routing algorithm works within and between domains.												
2.	It need to know only about other routers within their domain.	It need to know only about other routers within and between their domain.												
3.	Protocols used in intradomain routing are known as Interior-gateway protocols.	Protocols used in interdomain routing are known as Exterior-gateway protocols.												

4.	In this Routing, routing takes place within an autonomous network.	In this Routing, routing takes place between the autonomous networks.
	Intradomain routing protocols ignores the internet outside the AS(autonomous system).	Interdomain routing protocol assumes that the internet contains the collection of interconnected AS(autonomous systems).
	Some Popular Protocols of this routing are RIP(resource information protocol) and OSPF(open shortest path first).	Popular Protocols of this routing is BGP(Border Gateway Protocol) used to connect two or more AS(autonomous system).

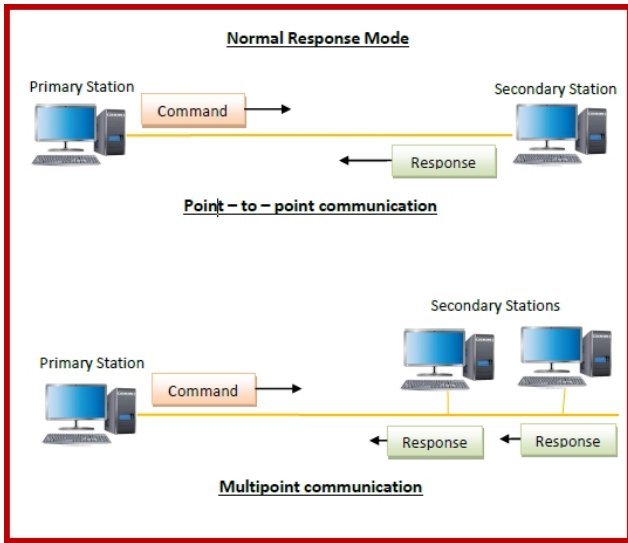
Implement Path vector routing with five nodes.

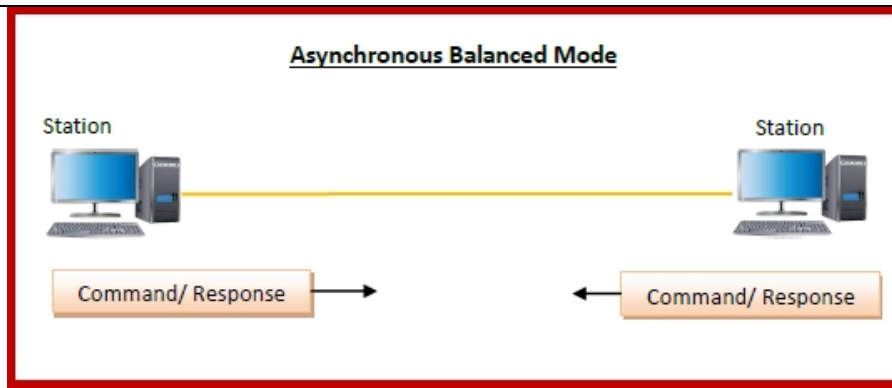


Distance vector and link state routing are both intradomain routing protocols. They can be used inside an autonomous system, but not between autonomous systems. These two protocols are not suitable for interdomain routing mostly because of scalability. Both of these routing protocols become intractable when the domain of operation becomes large. Distance vector routing is subject to

	<p>instability if there are more than a few hops in the domain of operation. Link state routing needs a huge amount of resources to calculate routing tables. It also creates heavy traffic because of flooding. There is a need for a third routing protocol which we call path vector routing.</p> <p>Node A1 is the speaker node for AS1, B1 for AS2, C1 for AS3, and D1 for AS4. Node A1 creates an initial table that shows A1 to A5 are located in AS1 and can be reached through it. Node B1 advertises that B1 to B4 are located in AS2 and can be reached through B1. And so on.</p>	
--	---	--

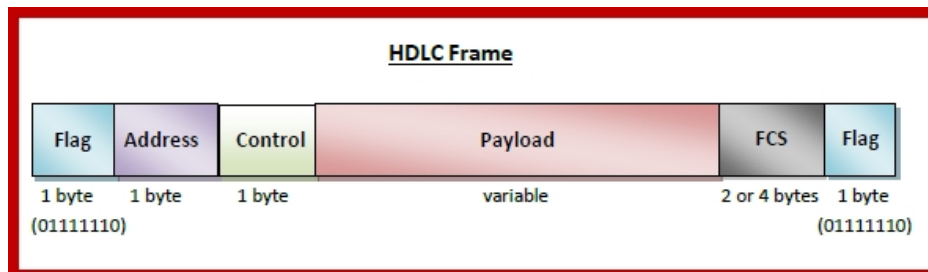
PART C (2x12 = 24)
ANSWER ANY ONE QUESTIONS

Q.No	Questions	Marks
17.a	<p>Analyze HDLC protocol modes of operation, Frames and Frame types</p> <p>HDLC supports two types of transfer modes, normal response mode and asynchronous balanced mode.</p> <p>Normal Response Mode (NRM) – Here, two types of stations are there, a primary station that send commands and secondary station that can respond to received commands. It is used for both point - to - point and multipoint communications.</p> <div style="text-align: center;">  <p>The diagram illustrates the Normal Response Mode (NRM) of HDLC. It is divided into two parts: 'Point-to-point communication' and 'Multipoint communication'. In the point-to-point part, a Primary Station (represented by a computer icon) sends a 'Command' (orange box) to a Secondary Station (represented by a computer icon), which then sends a 'Response' (green box) back. In the multipoint part, the Primary Station sends a 'Command' to multiple Secondary Stations (represented by computer icons), which then send 'Responses' back to the Primary Station.</p> </div> <p>Asynchronous Balanced Mode (ABM) – Here, the configuration is balanced, i.e. each station can both send commands and respond to commands. It is used for only point - to - point communications.</p>	12



HDLC Frame

HDLC is a bit - oriented protocol where each frame contains up to six fields. The structure varies according to the type of frame. The fields of a HDLC frame are –

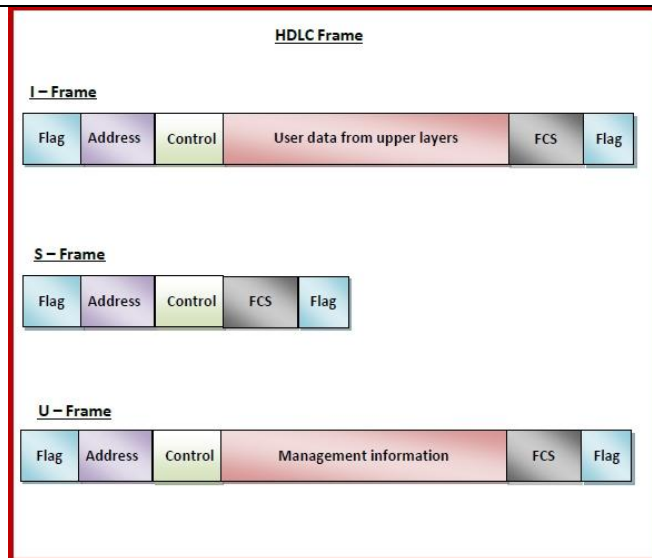


- **Flag** – It is an 8-bit sequence that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
- **Address** – It contains the address of the receiver. If the frame is sent by the primary station, it contains the address(es) of the secondary station(s). If it is sent by the secondary station, it contains the address of the primary station. The address field may be from 1 byte to several bytes.
- **Control** – It is 1 or 2 bytes containing flow and error control information.
- **Payload** – This carries the data from the network layer. Its length may vary from one network to another.
- **FCS** – It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code) (8)

Types of HDLC Frames

There are three types of HDLC frames. The type of frame is determined by the control field of the frame –

- **I-frame** – I-frames or Information frames carry user data from the network layer. They also include flow and error control information that is piggybacked on user data. The first bit of control field of I-frame is 0.
- **S-frame** – S-frames or Supervisory frames do not contain information field. They are used for flow and error control when piggybacking is not required. The first two bits of control field of S-frame is 10.
- **U-frame** – U-frames or Un-numbered frames are used for myriad miscellaneous functions, like link management. It may contain an information field, if required. The first two bits of control field of U-frame is 11.



(4)

(or)

Support how Sliding window protocol will be implemented in Go Back N and Selective Repeat protocol

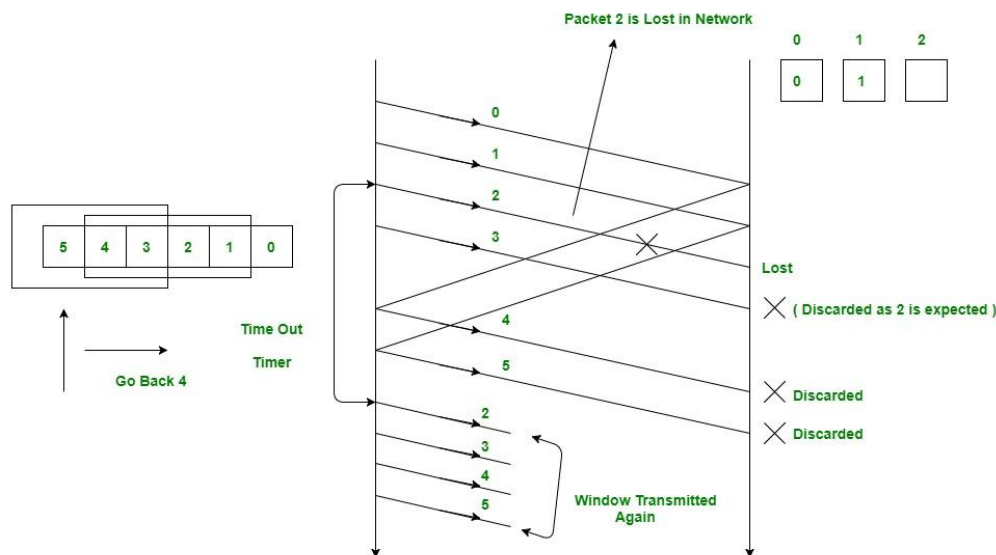
Go Back N (GBN) Protocol:

1. **Sender Window Size (WS)**

It is N itself. If we say the protocol is GB10, then $W_s = 10$. N should be always greater than 1 in order to implement pipelining. For $N = 1$, it reduces to Stop and Wait protocol.

2. **Receiver Window Size (WR) \rightarrow WR=1**

17.b



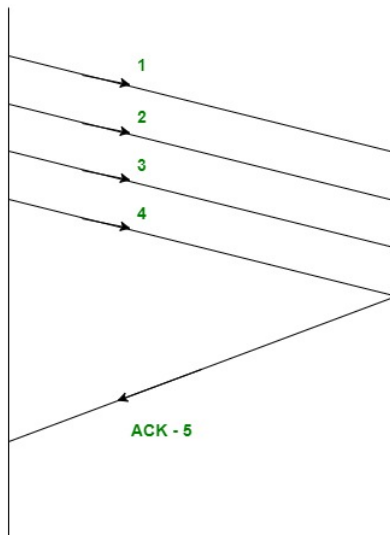
Assume window size of 4. Assume that we have lots of sequence numbers just for the sake of explanation. Now the sender has sent the packets 0, 1, 2 and 3. After acknowledging the packets 0 and 1, receiver is now expecting packet 2 and sender window has also slid to further transmit the packets 4 and 5. Now suppose the packet 2 is lost in the network, Receiver will discard all the packets which sender has transmitted after packet 2 as it is expecting sequence number of 2. On the sender side for every packet send there is a time out timer which will expire for packet number 2. Now from the last transmitted packet 5 sender will go back to the packet number 2 in the

current window and transmit all the packets till packet number 5. That's why it is called Go Back N. Go back means sender has to go back N places from the last transmitted packet in the unacknowledged window and not from the point where the packet is lost.

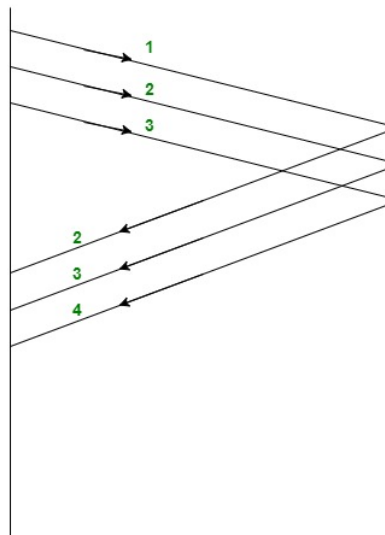
Acknowledgements

There are 2 kinds of acknowledgements namely:

- **Cumulative Ack:** One acknowledgement is used for many packets. The main advantage is traffic is less. A disadvantage is less reliability as if one ack is the loss that would mean that all the packets sent are lost.
- **Independent Ack:** If every packet is going to get acknowledgement independently. Reliability is high here but a disadvantage is that traffic is also high since for every packet we are receiving independent ack.



Cummulative



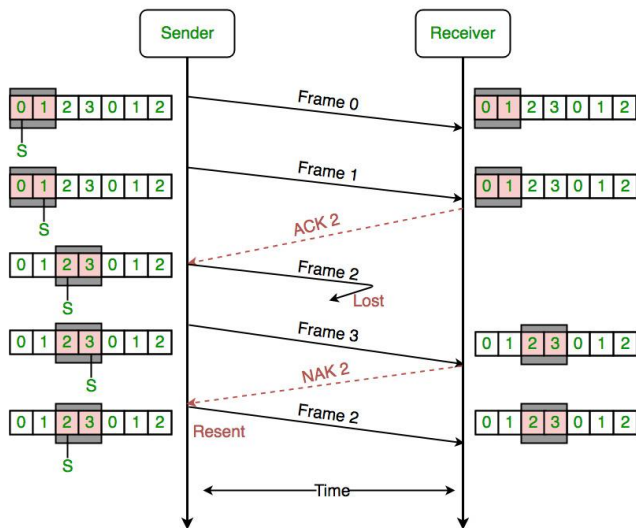
INDEPENDENT

-----**(6)**

Selective Repeat Protocol (SRP) :

This protocol(SRP) is mostly identical to GBN protocol, except that buffers are used and the receiver, and the sender, each maintain a window of size. SRP works better when the link is very unreliable. Because in this case, retransmission tends to happen more frequently, selectively retransmitting frames is more efficient than retransmitting all of them. SRP also requires full duplex link. backward acknowledgements are also in progress.

- Sender's Windows (Ws) = Receiver's Windows (Wr).
- Window size should be less than or equal to half the sequence number in SR protocol. This is to avoid packets being recognized incorrectly. If the windows size is greater than half the sequence number space, then if an ACK is lost, the sender may send new packets that the receiver believes are retransmissions.
- Sender can transmit new packets as long as their number is with W of all unACKed packets.
- Sender retransmit un-ACKed packets after a timeout – Or upon a NAK if NAK is employed.
- Receiver ACKs all correct packets.
- Receiver stores correct packets until they can be delivered in order to the higher layer.
- In Selective Repeat ARQ, the size of the sender and receiver window must be at most one-half of 2^m .

	 <p style="text-align: right;">-----(6)</p>	
18.a	<p>Demonstrate how EIGRP protocol overcomes the issues with IGP in accordance with the features of EIGRP.</p> <p>Enhanced Interior Gateway Routing Protocol (EIGRP) is a Cisco-proprietary hybrid routing protocol that contains features of distance-vector and link-state routing protocols. It is a network layer protocol which works on the protocol number 88.</p> <p>Some of its features are:</p> <ol style="list-style-type: none"> 1. Rapid convergence – EIGRP uses DUAL algorithm to support rapid convergence. If a route to a network goes down then another route(feasible successor) can be used. If there is no route present to that network in the topology table also then a query message is multicast to find out the alternative route to that network. 2. Reduced bandwidth usage – EIGRP doesn't send periodic updates like other distance vector routing protocol does.Distance Vector Routing protocol like RIP sends full routing table over a period of time therefore consumes the available bandwidth needlessly but EIGRP uses partial updates if there is any change in the topology occurs i.e updates are triggered only if any event occurs therefore consuming the bandwidth when needed. Also, EIGRP updates are propagated to the routers only who requires it. 3. Support all LAN and WAN data link protocols and typologies – EIGRP supports multi-access network like fddi, token ring etc and all WAN topologies like leased line, point-to-point links. EIGRP doesn't require any additional configuration across layer 2 protocols like frame relay. 	

4. **Supports auto-summary** – In EIGRP, auto-summarization is enabled by default. Auto summarization is a feature which allows Routing Protocols to summarize its routes to their classful networks automatically i.e routers will receive summarised routes automatically. EIGRP. e.g-1.1.1.1 /24 will be automatically summarised to the classful 1.1.1.1/8
5. **Supports unequal cost load balancing** – Unequal cost load balancing is possible in EIGRP by changing the value of variance. By default, variance is 1 therefore supports equal cost load balancing but if we want to use unequal cost load balancing then we can change the value of variance according to the amount of traffic we want to divide across different paths. Feasible distance is multiplied in such a way that it becomes greater than the value of feasible distance of successor.
6. **Communication via Reliable Transfer Protocol (RTP)** – EIGRP depends upon proprietary protocol RTP to manage the communication between EIGRP speaking routers. EIGRP uses 224.0.0.10 as its multicast address. For each multicast it sends, the router prepares and maintains a list of routers (speaking EIGRP). If no acknowledgement of multicast is received then same data is transmitted through 16 unicast messages. If no acknowledgement is received even after 16 unicast attempt then it is declared dead. This process is known as reliable multicast.
7. **Best path selection using DUAL** – EIGRP uses Diffusing Update Algorithm (DUAL) to find out the best path available to a network. EIGRP speaking routers maintains a topology table in which all the routes to the network are maintained. If the best path (successor) goes down, then second best path (feasible successor) is used from the topology table. If there is no path available in topology table then it sends a query message to resolve the query.

It maintains 3 different tables mainly:

(a) **Neighbor table:** It contains information about the routers with which neighbourhood has been formed. It contains the SRTT, RTP. It also contains queue count value for the hello messages that are not being acknowledged.

(b) **Topology table:** It contains all the routes available to a network (both feasible successor and successor).

(c) **Routing table:** It contains all the routes which are being used to make

current routing decisions. The routes in this table are considered as successor (best path) route -----(6)

EIGRP:

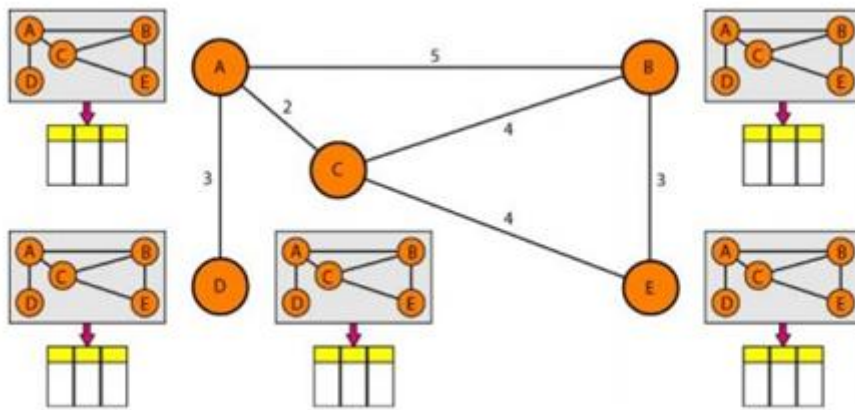
Enhanced Interior Gateway Routing Protocol (EIGRP) is a dynamic routing Protocol which is used to find the best path between any two layer 3 device to deliver the packet. EIGRP works on network layer Protocol of osi model and uses the protocol number 88. It uses metric to find out best path between two layer 3 device (router or layer 3 switch) operating EIGRP. Administrative Distance for EIGRP are:-

EIGRP ROUTES	AD VALUES
Summary Routes	5
Internal Routes	90
external routes	170

1. **Hello message**-These messages are keep alive messages which are exchanged between two devices operating EIGRP. These messages are used for neighbour discovery/recovery, if there is any device operating EIGRP or if any device (operating EIGRP) coming up again. These messages are used for neighbor discovery if multicast at 224.0.0.10. It contains values like AS number, k values etc. These messages are used as acknowledgment when unicast. A hello with no data is used as the acknowledgment.
2. **NULL update**-It is used to calculate SRTT (Smooth Round Trip Timer) and RTO (Retransmission Time Out).
SRTT: The time is taken by a packet to reach neighboring router and the acknowledgment of the packet to reach to the local router.

RTO: If a multicast fails then unicast are being sent to that router. RTO is the time for which the local router waits for an acknowledgment of the packet.
3. **Full Update** – After exchanging hello messages or after the neighbourship is formed, these messages are exchanged. This message contains all the best routes.
4. **Partial update**-These messages are exchanged when there is a topology

	<p>change and new links are added. It contains only the new routes, not all the routes. These messages are multicast.</p> <p>5. Query message-These messages are multicast when the device is declared dead and it has no routes to it in its topology table.</p> <p>6. Reply message – These messages are the acknowledgment of the query message sent to the originator of the query message stating the route to the network which has been asked in the query message.</p> <p>7. Acknowledgement message It is used to acknowledge EIGRP update, queries, and replies. Acks are hello packets that contain no data. Note:-Hello, and acknowledgment packets do not require any acknowledgment. Reply, query, update messages are reliable messages i.e requires acknowledgement. -----(6)</p>	
(or)		
18.b	<p>Design an network with any topology and construct routing table and explain Link state routing.</p> <p>Link State Routing –</p> <ul style="list-style-type: none"> • It is a dynamic routing algorithm in which each router shares knowledge of its neighbors with every other router in the network. • A router sends its information about its neighbors only to all the routers through flooding. • Information sharing takes place only whenever there is a change. • It makes use of Dijkstra's Algorithm for making routing tables. • Problems – Heavy traffic due to flooding of packets. – Flooding can result in infinite looping which can be solved by using Time to leave (TTL) field. 	



Link state routing has a different philosophy from that of distance vector routing. In link state routing, if each node in the domain has the entire topology of the domain the list of nodes and links, how they are connected including the type, cost (metric), and condition of the links (up or down)-the node can use Dijkstra's algorithm to build a routing table.

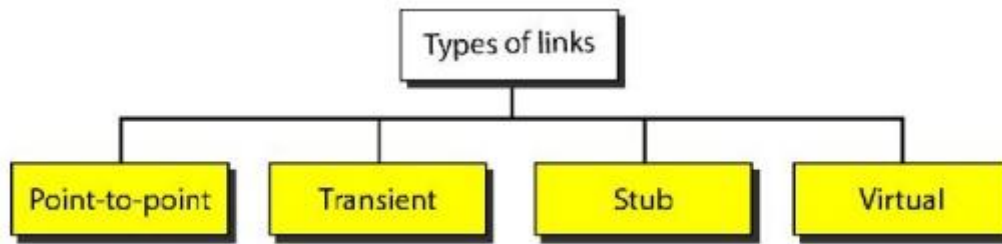
The figure shows a simple domain with five nodes. Each node uses the same topology to create a routing table, but the routing table for each node is unique because the calculations are based on different interpretations of the topology. This is analogous to a city map. While each person may have the same map, each needs to take a different route to reach her specific destination.-----(8)

Building Routing Tables:

In link state routing, four sets of actions are required to ensure that each node has the routing table showing the least-cost node to every other node.

- a) Creation of the states of the links by each node, called the link state packet (LSP).
- b) Dissemination of LSPs to every other router, called **flooding**, in an efficient and reliable way.
- c) Formation of a shortest path tree for each node.
- d) Calculation of a routing table based on the shortest path tree.

Types of Links



In OSPF terminology, a connection is called a *link*. Four types of links have been defined: point-to-point, transient, stub, and virtual.

A point-to-point link connects two routers without any other host or router in between. In other words, the purpose of the link (network) is just to connect the two routers. An example of this type of link is two routers connected by a telephone line or a T line. There is no need to assign a network address to this type of link. Graphically, the routers are represented by nodes, and the link is represented by a bidirectional edge connecting the nodes. The metrics, which are usually the same, are shown at the two ends, one for each direction. In other words, each router has only one neighbor at the other side of the link.-----**(4)**

Signature of the Faculty

HOD/CSE