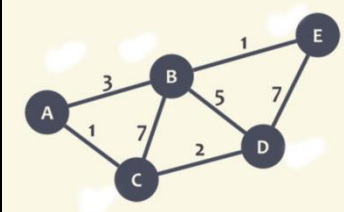


Scheme of Evaluation Internal
Assessment Test 2 – Dec 2022

Sub:	Computer Networks and Security					Code:	18CS52		
Date:	01/12/2022	Duration:	90mins	Max Marks:	50	Sem:	V	Branch:	ISE

Note: Answer Any five full questions.

Question #	Description	Marks Distribution	Max Marks
1	<p>a.</p>  <p>Find the shortest path from node A to all other nodes and construct the spanning tree in the above graph by Link state routing algorithm</p> <p>Identify as Dijkstras Algorithm Solve the graph and find spanning tree Find minimum cost Find minimum path</p>	<p>1M 6M 2M 1M</p>	10M
2	<p>Design a flow diagram for the protocol which retransmits only lost packet from the last ACK after timeout event.</p> <p>Identify its SR protocol Flow diagram with proper convention Explanation</p>	<p>1M 7M 2M</p>	10M
a	<p>Explain the process of transition from IPv4 to IPv6 with an example diagram</p> <p>Two methods: Dual stack and tunneling</p>	2M	

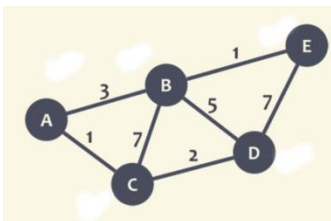
3		Explanation	2.5M each	10M	10M
4	a)	Explain about how IP address is allocated randomly to a device as soon as internet is turned on.	7M		
		Explain about steps involved in communication via Virtual Circuit Network (VCN) in network layer.	3M		
		Identify its working mechanism of DHCP server Explain DHCP with neat flow diagram	1M 6M	7M	
		VCN network configuration Routing table filling and VCI	2M 1M		10M
	b)			3M	
5	a)	Design communication flow for reliable data transfer in following situations (i) Retransmission due to lost ACK. (ii) Sending multiple packets back-to-back. (iii) Avoiding retransmission by cumulative ACK. (iv) Fast retransmit. (v) Slow start.	10M	10M	10M
		Each situation explain with flow diagram	2M	10M	
6		Draw and explain IPv6 datagram format. List and describe input and out ports in switch.	7M 3M	7M	
		IPv6 packet format Explain each field	3M 4M		10M
		Diagram	1M	3M	
		Input Port	1M		
		Output port	1M		

Scheme Of Evaluation Internal Assessment Test 2 – Dec 2022

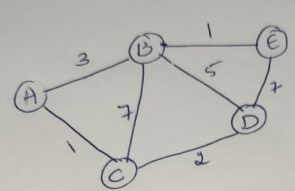
Sub:	Computer Networks and Security					Code:	18CS52
Date:	01/12/2022	Duration:	90mins	Max Marks:	50	Sem:	V
						Branch:	ISE

Note: Answer Any full five questions

Q1.



Find the shortest path from node A to all other nodes and construct the spanning tree in the above graph by Link state routing algorithm.



Dijkstra's Algorithm

	A	B	C	D	E
A	0	∞	∞	∞	∞
C	3	1	∞	∞	∞
B	7	3	3	∞	∞
D	5	3	3	4	∞
E	1	5	7	4	4

Source A - B minimum cost 3

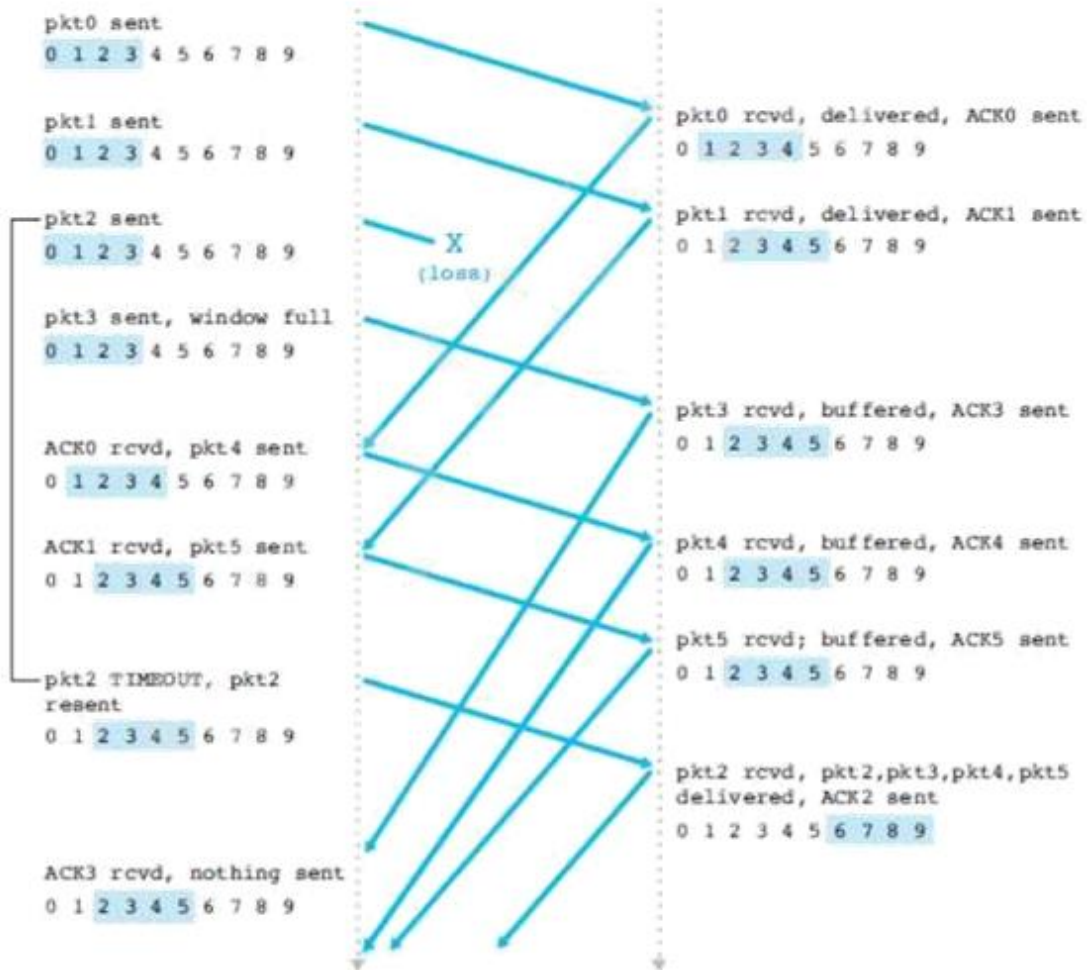
 A - C 1

 A - D 3

 A - E 4

Q2. Design a flow diagram for the protocol which retransmits only lost packet from the last ACK after timeout event.

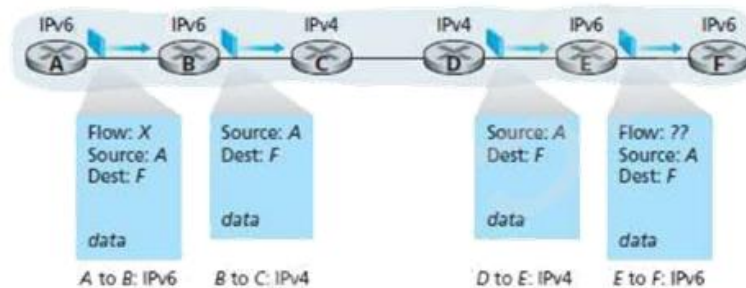
It is selective repeat protocol.



Q3. Explain the process of transition from IPv4 to IPv6 with an example diagram.

3.4.5.5.1 Dual Stack Approach

- IPv6-capable nodes also have a complete IPv4 implementation. Such nodes are referred to as IPv6/IPv4 nodes.
- IPv6/IPv4 node has the ability to send and receive both IPv4 and IPv6 datagrams.
- When interoperating with an IPv4 node, an IPv6/IPv4 node can use IPv4 datagrams.
 - When interoperating with an IPv6 node, an IPv6/IPv4 node can use IPv6 datagrams.
- IPv6/IPv4 nodes must have both IPv6 and IPv4 addresses.
- IPv6/IPv4 nodes must be able to determine whether another node is IPv6-capable or IPv4-only.
- This problem can be solved using the DNS.
 - If the node name is resolved to IPv6-capable, then the DNS returns an IPv6 address
 - Otherwise, the DNS return an IPv4 address.
- If either the sender or the receiver is only IPv4-capable, an IPv4 datagram must be used.
- Two IPv6-capable nodes can send IPv4 datagrams to each other.



- Here is how it works:
 - 1) Suppose IPv6-capable Node-A wants to send a datagram to IPv6-capable Node-F.
 - 2) IPv6-capable Node-B creates an IPv4 datagram to send to IPv4-capable Node-C.
 - 3) At IPv6-capable Node-B, the IPv6 datagram is copied into the data field of the IPv4 datagram and appropriate address mapping can be done.
 - 4) At IPv6-capable Node-E, the IPv6 datagram is extracted from the data field of the IPv4 datagram.
 - 5) Finally, IPv6-capable Node-E forwards an IPv6 datagram to IPv6-capable Node-F.
- Disadvantage: During transition from IPv6 to IPv4, few IPv6-specific fields will be lost.

3.4.5.5.2 Tunneling

- Tunneling is illustrated in Figure 3.21.
- Suppose two IPv6-nodes B and E
 - want to interoperate using IPv6 datagrams and
 - are connected by intervening IPv4 routers.
- The intervening-set of IPv4 routers between two IPv6 routers are referred as a tunnel.
- Here is how it works:
 - On the sending side of the tunnel:
 - IPv6-node B takes & puts the IPv6 datagram in the data field of an IPv4 datagram.
 - The IPv4 datagram is addressed to the IPv6-node E.
 - On the receiving side of the tunnel: The IPv6-node E
 - receives the IPv4 datagram
 - extracts the IPv6 datagram from the data field of the IPv4 datagram and
 - routes the IPv6 datagram to IPv6-node F



Q3 Differentiate between IPv4 and IPv6 in communication

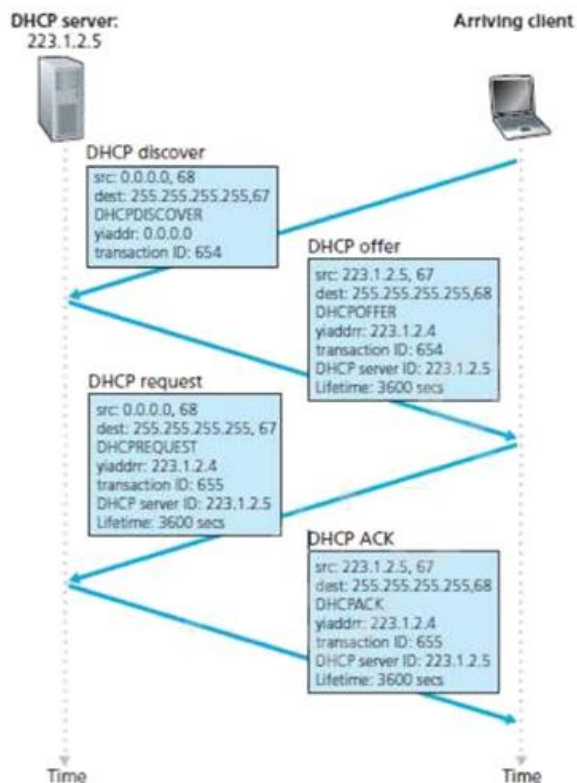
3.4.5.4 Difference between IPv4 & IPv6

	IPv4	IPv6
1	IPv4 addresses are 32 bit length	IPv6 addresses are 128 bit length
2	Fragmentation is done by sender and forwarding routers	Fragmentation is done only by sender
3	Does not identify packet flow for QoS handling	Contains Flow Label field that specifies packet flow for QoS handling
4	Includes Options up to 40 bytes	Extension headers used for optional data
5	Includes a checksum	Does not includes a checksum
6	Address Resolution Protocol (ARP) is available to map IPv4 addresses to MAC addresses	Address Resolution Protocol (ARP) is replaced with Neighbor Discovery Protocol (NDP)
7	Broadcast messages are available	Broadcast messages are not available
8	Manual configuration (Static) of IP addresses or DHCP (Dynamic configuration) is required to configure IP addresses	Auto-configuration of addresses is available
9	IPSec is optional, external	IPSec is required

Q4 Explain about how IP address is allocated randomly to a device as soon as internet is turned on.

3.4.3.4.1 DHCP Protocol

- DHCP enables auto-configuration of IP address to host.
- DHCP assigns dynamic IP addresses to devices on a network.
- Dynamic address allocation is required
 - when a host moves from one network to another or
 - when a host is connected to a network for the first time.



• Four steps in DHCP protocol (Figure 3.16):

1) DHCP Server Discovery

- DHCP server contains a range of unassigned addresses to be assigned to hosts on-demand.
- To contact DHCP server, a client broadcasts a DHCPDISCOVER message with destination IP address 255.255.255.255.

2) DHCP Server Offer

- DHCP server broadcasts DHCP OFFER message containing
 - client's IP address
 - network mask and
 - IP address lease time (i.e. the amount of time for which the IP address will be valid).

3) DHCP Request

- The client sends a DHCPREQUEST message, requesting the offered address.

4) DHCP ACK

- The DHCP server acknowledges with a DHCPACK message containing the requested configuration.

Q4 Explain about steps involved in communication via Virtual Circuit Network (VCN) in network layer.

3.2.1 Virtual Circuit Networks

- A VC consists of
 - 1) A path between the source and destination.
 - 2) VC number: This is one number for each link along the path.
 - 3) Entries in the forwarding-table in each router.
- A packet belonging to a virtual-circuit will carry a VC number in its header.
- At intervening router, the VC number of traversing packet is replaced with a new VC number.
- The new VC number is obtained from the forwarding-table.

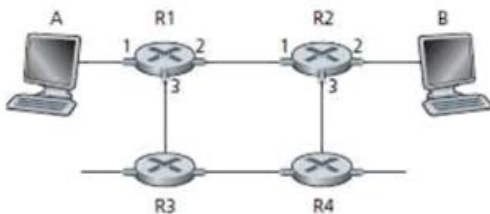


Figure 3.2: A simple virtual-circuit network

Incoming Interface	Incoming VC #	Outgoing Interface	Outgoing VC #
1	12	2	22
2	63	1	18
3	7	2	17
1	97	3	87

Table 3.1: Forwarding-table in R1

Q5. Design communication flow for reliable data transfer in following situations

- (i) Retransmission due to lost ACK.
- (ii) Sending multiple packets back-to-back.
- (iii) Avoiding retransmission by cumulative ACK.
- (iv) Fast retransmit.
- (v) Slow star

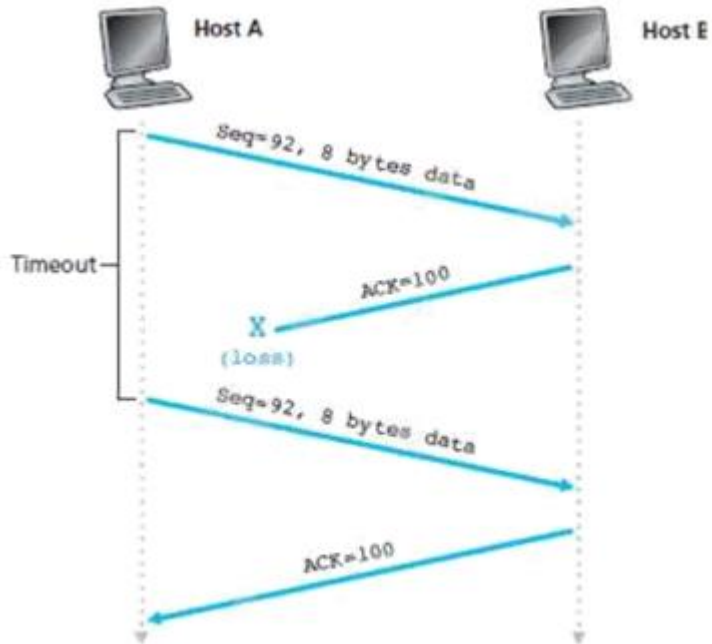


Figure 2.28: Retransmission due to a lost acknowledgment

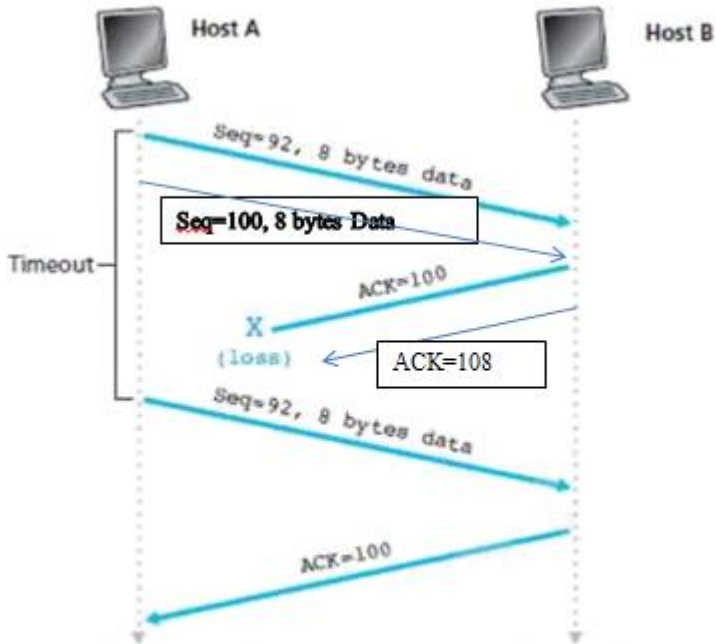


Figure 2.29: Segment 100 not retransmitted

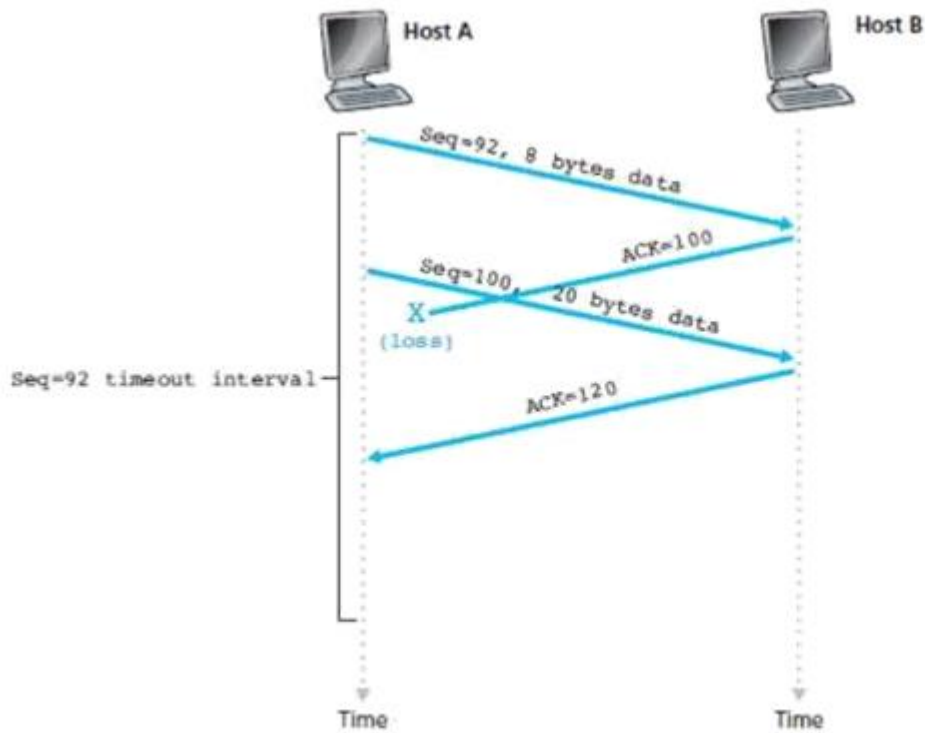


Figure 2.30: A cumulative acknowledgment avoids retransmission of the first-segment

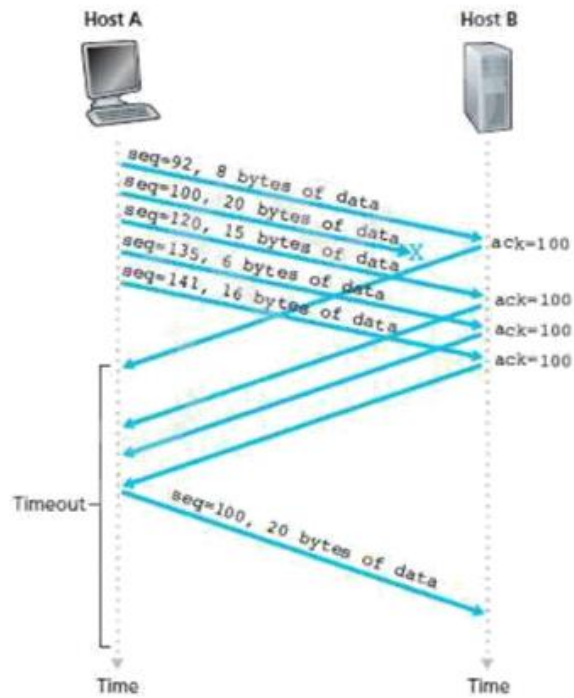


Figure 2.31: Fast retransmit: retransmitting the missing segment before the segment's timer expires

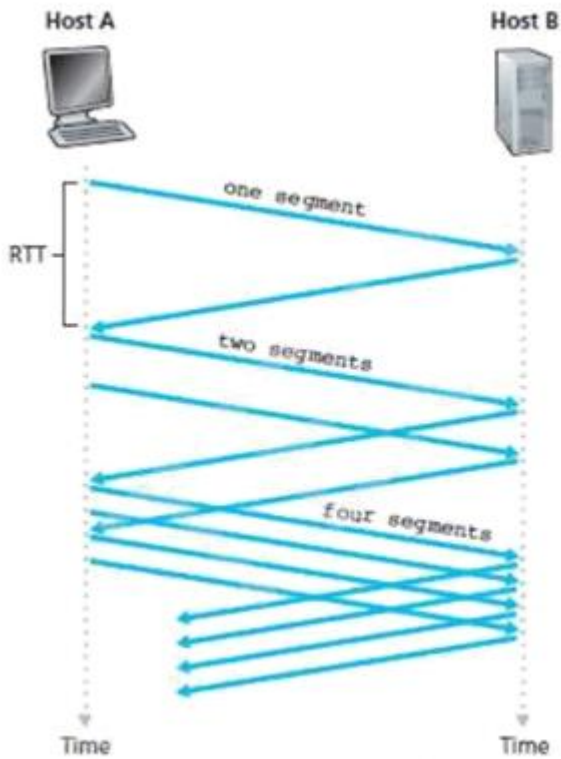


Figure 2.42: TCP slow start

Q6 Draw and explain IPv6 datagram format.

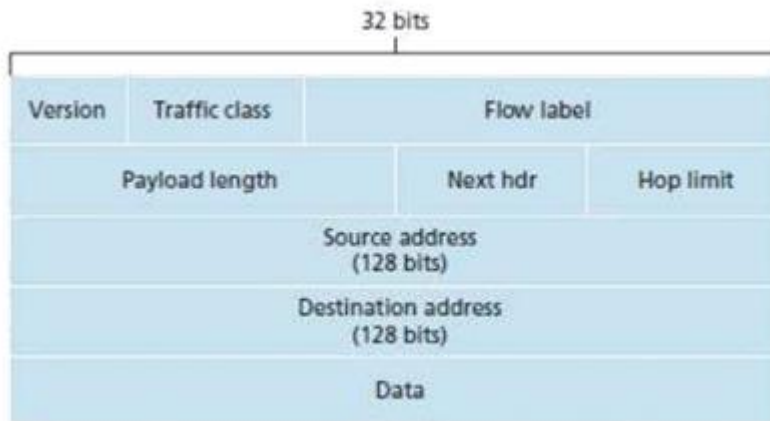


Figure 3.18: IPv6 datagram format

- The following fields are defined in IPv6:

1) Version

➤ This field specifies the IP version, i.e., 6.

2) Traffic Class

➤ This field is similar to the TOS field in IPv4.

➤ This field indicates the priority of the packet.

3) Flow Label

➤ This field is used to provide special handling for a particular flow of data.

4) Payload Length

➤ This field shows the length of the IPv6 payload.

5) Next Header

➤ This field is similar to the options field in IPv4 (Figure 3.19).

➤ This field identifies type of extension header that follows the basic header.

6) Hop Limit

➤ This field is similar to TTL field in IPv4.

➤ This field shows the maximum number of routers the packet can travel.

➤ The contents of this field are decremented by 1 by each router that forwards the datagram.

➤ If the hop limit count reaches 0, the datagram is discarded.

7) Source & Destination Addresses

➤ These fields show the addresses of the source & destination of the packet.

8) Data

➤ This field is the payload portion of the datagram.

➤ When the datagram reaches the destination, the payload will be

→ removed from the IP datagram and

→ passed on to the upper layer protocol (TCP or UDP).

Q6. List and describe input and out ports in switch.

1) Input Ports

- An input-port is used for terminating an incoming physical link at a router (Figure 3.6).
- It is used for interoperating with the link layer at the other side of the incoming-link.
- It is used for lookup function i.e. searching through forwarding-table looking for longest prefix match.
- It contains forwarding-table.
- Forwarding-table is consulted to determine output-port to which arriving packet will be forwarded.
- Control packets are forwarded from an input-port to the routing-processor.
- Many other actions must be taken:
 - i) Packet's version number, checksum and time-to-live field must be checked.
 - ii) Counters used for network management must be updated.

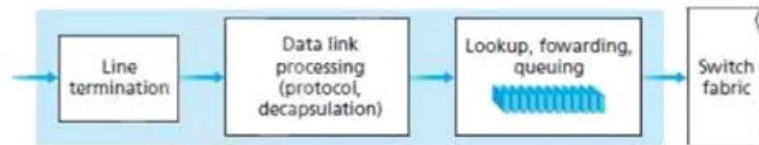


Figure 3.6: Input port processing

3.3.2 Output Processing

- Output-port processing
 - takes the packets stored in the output-port's memory and
 - transmits the packets over the output link (Figure 3.8).
- This includes
 - selecting and dequeuing packets for transmission and
 - performing the linklayer and physical-layer transmission functions.

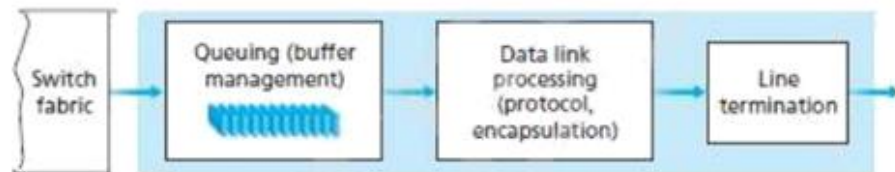


Figure 3.8: Output port processing