COMPUTER NETWORKS

Page No.
Date / /

Unit-3 Network Layer

One Shot + 3 PYQ Solutions

Topics :-

1. Network layer functions
2. Point to Point Network & logical Addressing
3. Basic Internetworking [IP, CIDR, ARP, DHCP, ICMP]
→ 4. Subnetting + 2021-22 10 marks numerical.
+ 2022-23 - 18-19 10 marks numerical.
5. IP Adressing and its class classification.
→ 6. IPv4 & IPV6
7. IPv6 advantages over IPv4 - 2018-19 [10 marks].
→ 8. IPV6 Vs IPv4 - 2022-23 [10 marks]
→ 9. ICMP - 2021-22 - [10 marks]
→ 10. Routing [Static & Dynamic]
11. Forwarding & Delivery.
→ 12. Routing Algorithms [Imp - DVR] 2021-22
→ 13. Congestion Control - [2017-18]
→ 14. QoS [Quality of Service] - [2018-19]
15. Congestion Control Algorithms.

Page No.:
Date: / /

Network Layer

- The Network Layer is the third layer of the OSI Model.
- It handles the service requests from the transport layer and further forwards the service requests from the transport layer and for to the data link layer.
- The network layer translates the logical addresses into the physical addresses.
- It determines the route from the source to the destination and also manages the traffic problems such as switching, routing and controls the congestion of data packets.
- The main role of the network layer is to move the packets from sending host to the receiving host.

Main functions performed by the network layer

1. Routing
2. Logical Addressing
3. Internetworking
4. Fragmentation.

Page No.
Date: / /

Point to Point Network

→ A point to point network is a permanent link between two end points.
→ A point to point connection provides a dedicated link between two devices.
→ link can be wire, microwave or satellite link.
→ The entire capacity of the link is reserved for transmission between two devices.
→ Uses different types of topology (mesh or star) to connect two internet nodes.

AKTU-[2021-22] 2marks

Q. Discuss the role logical addressing

→ For different level of communication, we need a global addressing scheme known as logical addressing.
→ An IP address is used globally to refer to the logical address in the network layer of the TCP/IP protocol.
→ An IPV4 address is a 32 bit address that uniquely and universally defines the connection of a device to the Internet.

Page No.:
Date:

* Basic Internetworking [IP, CIDR, ARP, DHCP, ICMP]

→ Internetworking is the process of connecting different networks by using intermediary devices such as routers or gateway devices.

→ It ensures data communication among networks owned & operated by different entities using a common data communication and the Internet Routing Protocol.

→ Internetworking is only possible when all the connected networks use the same protocol stack.

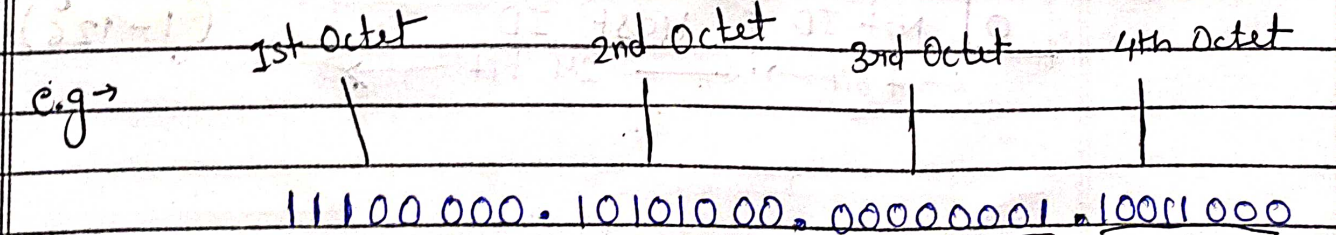
* IP Addressing

→ It is the process of finding unique IP address. A unique IP address is required for each host and network component that communicates using TCP/IP.

→ It is a network layer address and has no dependence on the data link layer address.

IP Address Classes:

→ The 32-bit IP address contains information about the host and its network.



Page No.
Date: / /

- Routers use Subnet Mask, which is as long as the size of the network address in the IP address. (32 bit)
- IP address (Binary) AND with its Subnet Mask result will Networks Address.

for example ⇒

IP Address : 192.168.1.152
Subnet Mask : 255.255.255.0 then :

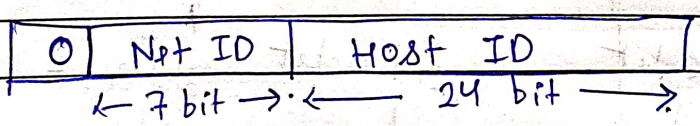
IP	11000000	10101000	00000001	10011000
Mask	11111111	11111111	11111111	00000000
Network	11000000	10101000	00000001	00000000

IP Address = no. of Networks + no. of hosts

No. of networks = $2^{\text{network\_bits}}$
No. of Hosts = $2^{\text{host-bits}} - 2$

1. Class A

The first bit always set to 0.

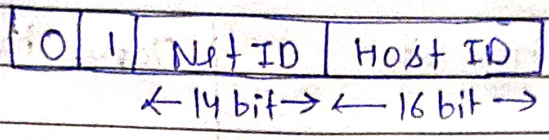


1st Octet (1-126)

Page No.:
Date:

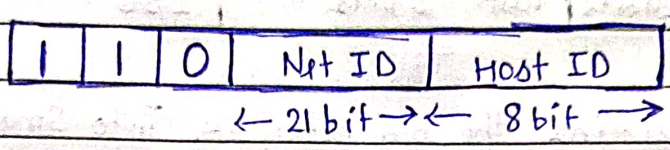
2. Class B

1st Octet
(128 - 191)



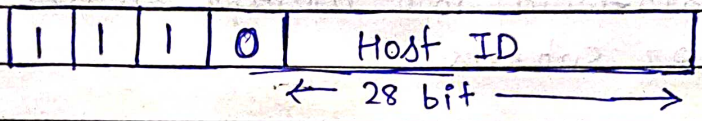
3. Class C

1st Octet
(192 - 223)



4. Class D

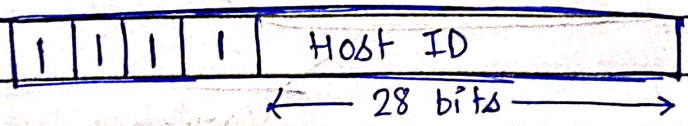
1st Octet
(224 - 239)



In Class D, an IP address is reserved for multicast addresses. It does not possess subnetting. The higher order bits of the first Octet is always set to 1110, and the remaining bits determines the host ID in any network.

5. Class E

In Class E, an IP address is used for the future use or for the research and development purposes. It does not possess any subnetting.



* Classful Network Architecture

Class	Higher bits	Network address bits	Host address bits	No. of networks	No.of hosts per network	Range
A	0	8	24	2^7	2^{24}	0.0.0.0 to 125.255.255.255
B	10	16	16	2^{14}	2^{16}	128.0.0.0 to 191.255.255.255
C	110	24	8	2^{21}	2^8	192.0.0.0 to 223.255.255.255
D	1110	Not defined and reserved for future	Not defined and reserved for future	Not defined and reserved for future	Not defined and reserved for future	224.0.0.0 to 239.255.255.255
E	1111	Not defined and reserved for future	Not defined and reserved for future	Not defined and reserved for future	Not defined and reserved for future	240.0.0.0 to 255.255.255.255

Page No.
Date: / /

Default Subnet Mask

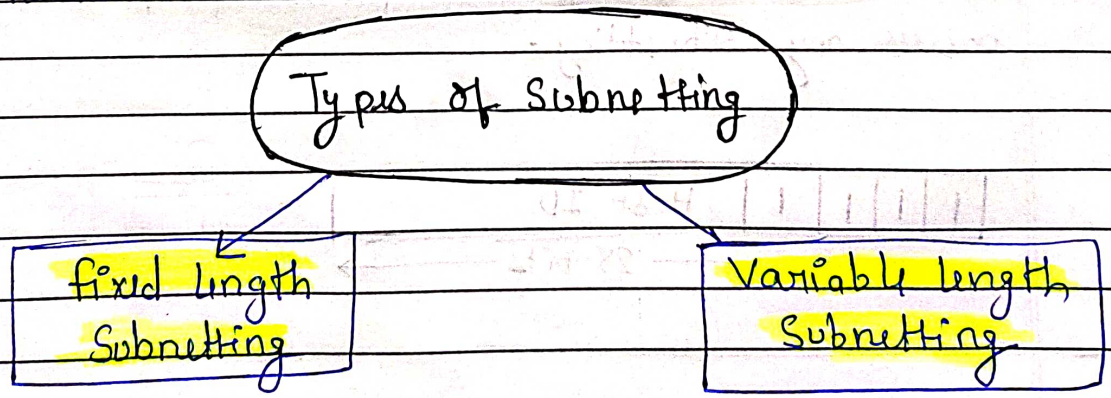
IP Class	Default Subnet	Network bits	Host bits	Total hosts
A	255.0.0.0	first 8 bits	last 24 bits	16,777,216
B	255.255.0.0	first 16 bits	last 16 bits	65,536
C	255.255.255.0	first 24 bits	last 8 bits	256

* **Subnetting** (Dividing the big network into small network)

It is a technique in which a single physical network is logically partitioned into multiple smaller subnetworks or subnets

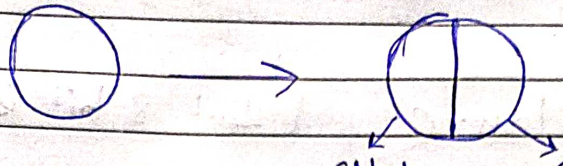
Advantages
- It improves the security
- The maintenance and administration of subnet is easy.

Disadvantages
- Identification of a station is difficult.
- Not possible to directed broadcast from outside network.



Page No.:
Date: / /

Q. Consider the network having IP Address 200.1.2.0. Divide this network into two Subnets.



200.1.2.0 0 0 0 0 0 0 0 ← 25 →

200.1.2.1 0 0 0 0 0 0 0 ← 25 →

(127) 0 1 1 1 1 1 1 1

(128) (255) 1 1 1 1 1 1 1 1

1st Subnet	2nd Subnet
• IP Address of the Subnet = 200.1.2.0 (Reserved)	• IP Address of the Subnet = 200.1.2.128 (Reserved)
• Direct Broadcast Address = 200.1.2.127 (Reserved)	• Direct Broadcast Address = 200.1.2.255 (Reserved)
• Total number of IP Addresses = $2^7 = 128$	• Total number of IP Addresses = $2^7 = 128$
• Range = [200.1.2.0, 200.1.2.127]	• Range = [200.1.2.128, 200.1.2.255]
• Total no. of host = 128 - 2 = 126	• Total no. of host = 128 - 2 = 126
• Range of Allocated IP Addresses = [200.1.2.1, 200.1.2.126]	• Range of Allocated IP Addresses = [200.1.2.129, 200.1.2.254]

Page No.
Date / /

AKTU- 2021-22 [10 marks]

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

Ans 200.1.2.0 → class-C [last 8 bit is host]

00 000000
00 111111

200.1.2.0 - 200.1.2.63
1st subnet

01 000000
01 111111

200.1.2.64 - 200.1.2.127
2nd subnet

10 000000
10 111111

200.1.2.128 - 200.1.2.191
3rd subnet

110 00000
110 11111

200.1.2.192 - 200.1.2.223
4th subnet

111 00000
111 11111

200.1.2.224 - 200.1.2.255
5th subnet

→ 00
→ 01
→ 10
→ 11 → 110, 111

Page No.:
Date: / /

AKTU - [2022-23, 2018-19] [10 marks]

Q. The IP network 200.198.160.0 is using subnet mask 255.255.255.224. Draw the subnets.

Ans. Step 1st = IP – Binary = 200.198.160.0
= 11001000.11000110.10100000.00000000

2. Step 2nd = Inverse Subnet mask = 255.255.255.224 = 0.0.0.31

3. Step 3rd Broad cast Address = (IP) logical OR (Inverse Subnet)

(IP) = 11001000.11000110.10100000.00000000
OR (Inverse) 00000000.00000000.00000000.00011111
= 11001000.11000110.10100000.00011111

4. Broad cast Address = 200.198.160.31.

5. Range of Subnet Mask = 0 – 31

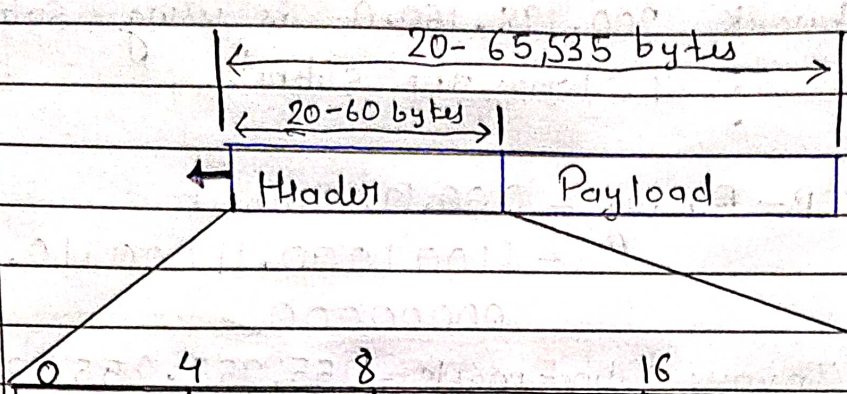
6. Draw Subnets.

1st Subnet =	200.198.160. 0	—	200.198.160. 31	.
2nd Subnet =	"	.32 –	"	.63 .
3rd Subnet =	"	.64 –	"	.95
4th Subnet =	"	.96 –	"	.127
5th Subnet =	"	.128 –	"	.159
6th Subnet =	"	.160 –	"	.191
7th Subnet =	"	.192 –	"	.223
8th Subnet =	"	.224 –	"	.255

Total = 8 Subnet

Page No.
Date / /

IPv4



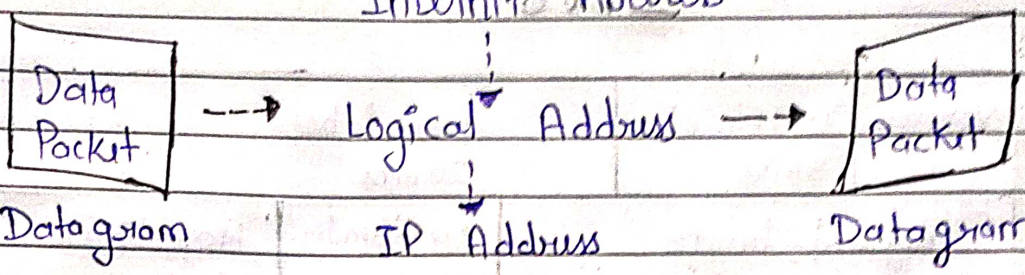
0	4	8	16	31
VER (4 bits)	HLEN (4 bits)	Service type (8 bits)	Total length (16 bits)	
Identification (16 bits)			Flags (3 bits)	Fragmentation offset (13 bits)
Time-to-live (8 bits)		Protocol (8 bits)	Header checksum (16 bits)	
Source IP address (32 bits)				
Destination IP address (32 bits)				
Options + Padding (0 to 40 bytes)				

→ An IPv4 datagram consist of a header section and data section.
→ IPv4 header contains 13 fields of which 12 always requested, but 13th is optional.
→ fields in the header are packed in left to right and top to down fashion with MSB comes first.

① **Version** = which version of IP (4/6)

② **Header** = because header length is variable.

Page No.:
Date:



IPv4 address --> 32 bit ---> 2^{32} addresses
IPv6 address --> 128 bit ---> 2^{128} addresses

③ **Services** : used to define priority and special demands like delay throughput, reliability, cost etc.

④ **Total length** = total datagram = header + data.

⑤ **Identification** : used to identify a datagram uniquely.

⑥ **Flags** : Do not fragment, More fragments.

⑦ **Fragmentation offset** : used in case of fragmentation, how many bits before current packet.

⑧ **Time to live** : maximum hops after which packet will be discarded.

⑨ **Protocol** : the protocol for which it is carrying the payload.

⑩ **Header checksum** : for user check but confined to header only.

⑪ **Source Address** : Sets the source IP Address.

⑫ **Destination Address** : An indicating the receiver of the packet.

Page No.
Date: / /

IPv6

Version 4bits	Traffic class 8bits	Flow label 20 bits	
Payload length 16bits		Next header 8 bits	Hop limit 8 bits
Source address 128 bits			
Destination address 128 bits			

→ IPv6 is the most recent version of the Internet Protocol, designed to succeed IPv4.

→ IPv6 was developed to address the exhaustion of available IPv4 addresses and to provide additional features and improvements over IPv4.

- **Version** (4bits): It represents the IP version number.
- **Traffic Class** (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of service to let the Router known what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN).

Page No.:
Date : / /

- **Flow Label (20 bits):**
→ An identifier of a flow of packets between a source & destination.
→ The label 0 means the packet does not belong to any flow.

- **payload length (16 bits):**
→ The size of the payload in octets, including any extension headers.

- **Next header (8 bits):** It specifies the type of the next header.

- **Hop limit (8 bits):** It replaces the Time To Live field in IPv4.

AKTU- 2018-19 [10 marks]

Q. Write advantages of Next-generation IPv6 over IPv4.

1. Larger Address Space = IPv6's 128 bit addresses offer an immense pool of unique addresses.

2. Efficient Routing = IPv6's simplified header improves routing efficiency and network management.

3. Built-in Security = Enhancing security without additional layers.

4. Enhanced Mobility = IPv6 supports mobile devices better.

5. Future-Proofing = designed to accommodate the continued growth of the Internet.

Page No.
Date / /

AKTU - 2022-23 [10 marks]

Q. Illustrate the difference between IPv4 and IPv6.

IPv6	IPv4
→ IPv6 has 128-bit address length	→ IPv4 has 32-bit address length.
→ It supports Auto and renumbering address configuration	→ It supports Manual and DHCP address configuration.
→ 3.4×10^{38} Address space	→ 4.29×10^{9} address space
→ Address Representation is in Hexadecimal (:)	→ Address Representation is in decimal. (.)
→ Checksum field is not available	→ checksum field is available.
→ IPv6 has a header of 40 bytes fixed.	→ IPv4 has a header of 20-60 bytes.
→ It does not support VLSM	→ It support VLSM (variable length subnet mask).

Page No.:
Date: / /

[IP, CIDR, ARP, RARP, DHCP, ICMP]

- **IP** → stands for Internet Protocol. It's set of rules governing the format of data sent over the Internet. IP addresses are unique identifiers assigned to each device on a network. e.g → 192.255.255.255.

- **CIDR** → stands for Classless Inter-Domain Routing. It's method for allocating IP addresses and routing IP packets more efficiently. CIDR notation is used to specify a range of IP addresses by combining the IP address with its Subnet mask. e.g ⇒ 192.255.255.255/12. ↑ N/w id

- **ARP** → stands for Address Resolution Protocol. used to find the MAC address of the destination. The purpose of ARP is to resolve an IPv4 address to the corresponding physical Address. IP ⟶ MAC

- **RARP** → stands for Reverse Address Resolution Protocol. we find IP address using RARP. RARP is a TCP/IP protocol that is responsible for the translation of MAC address to be translated into an IP address. MAC ⟶ IP

- **DHCP** → stands for Dynamic Host Configuration Protocol. The DHCP is controlled by a DHCP server that dynamically distributes network configuration parameters for interfaces and services. A DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks.

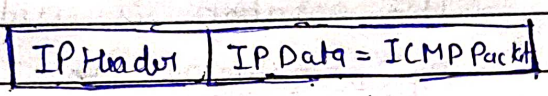
Page No.
Date / /

HRTU 2021-22 [6th sem]

- ICMP - Internet Control Message Protocol.

→ IP is an unreliable service, Here we don't forward an ack. for confirmation of frame reception.

→ ICMP is a Network layer protocol, that operates on Internet Protocol.
→ It is used for error reporting and diagnostic purposes



IP Packet.

→ ICMP is not a mandatory protocol in computer network
→ mainly used for reporting errors and management queries.

* Error Reporting : ✓

1. Source quench message:
→ when sender resends the packet at a higher rate and the router is not able to handle.
→ then router sends a SQM to sender to send the packet at a lower rate.

2. Time excided message:
→ when time-to-live value to Zero. then router discards a datagram and sends the TEM message to the original source.

Page No.:
Date: / /

3. Parameter Problem:
→ Incase of mismatch of calculated header checksum, packet will be dropped by the router and informs to the source by sending a PPM.

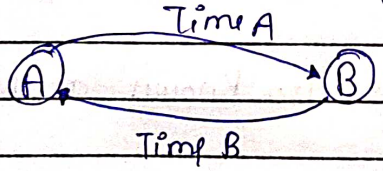
4. Destination un-reachable:
→ DU is generated by the host to inform the client that the destination is unreachable for some reason.

5. Redirection Message:
→ Redirect requests data packets are sent on an alternate route. The message informs a host to update its routing information.

* Query Management:

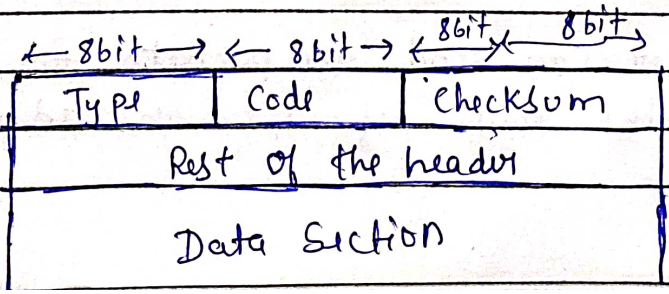
1. Echo Request & Reply:
→ It is used for diagnostic purpose whether two hosts can communicate with each other.

2. Timestamp Request and Reply:
→ used to calculated Round Trip Time.



$$\frac{\text{Time A} + \text{Time B}}{2} = \text{Timestamp}$$

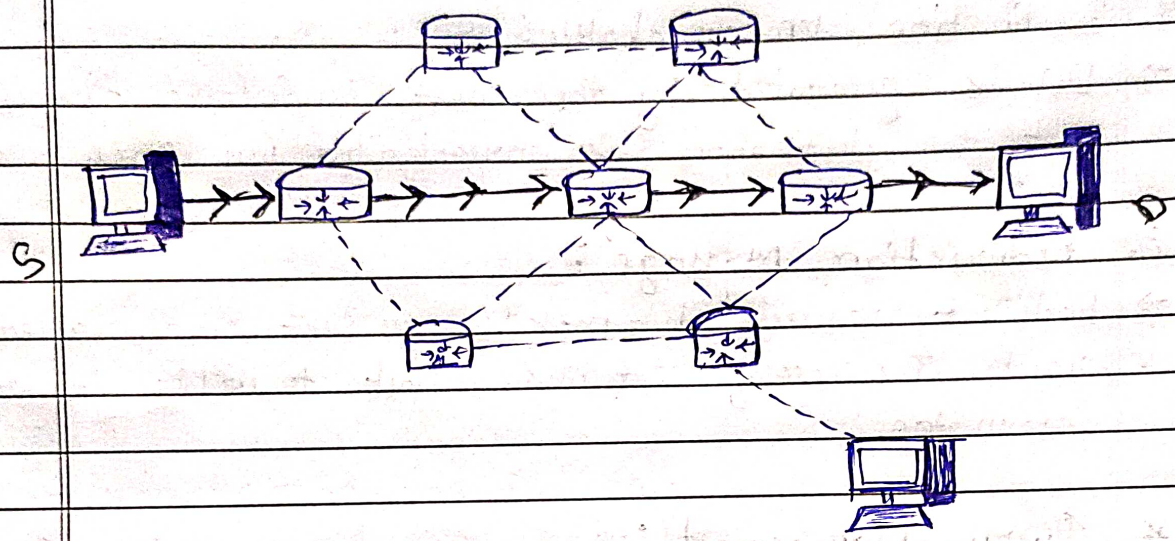
Format of ICMP



Page No.
Date / /

Routing

→ It is a process of selecting path along which the data can be transferred from source to destination



→ Routing is performed by a special device known as a router.

→ The routing algorithms are used for routing the packets. The routing algo. responsible for choosing the optimal path.

Static Routing

→ Static Routing is also known as Non-adaptive Routing.

→ It is a technique in which the administrator manually adds the routes in a routing table.

→ A Router can send the packets for the destination along the route defined by the administrator.

Page No.:
Date : / /

Adv ⇒ The cheaper router can be used to obtain static routing.
⇒ It provide security as the system administrator is allowed only to have control.

Disadv ⇒ Very difficult for large network.
⇒ The system administrator should have a good knowledge of a topology.

⇒ **Dynamic Routing**

→ It is also known as Adaptive Routing.

→ It is a technique in which a router adds a new route in the routing table for each packet in the condition of the network.

→ In Dynamic Routing, RIP and OSPF are the protocols used to discover the new routes.

Adv ⇒ It is easy to configure.
It is effective in selecting the best route.

Disadv ⇒ It is less secure.
⇒ It is more expensive.

Page No.
Date: / /

Forwarding

→ It is simply defined as the action applied by each router when a packet arrives at one of its interfaces. When a router receives a packet from one of its attached networks, it needs to forward the packet to another attached network.

1. Next hop Method:

→ One technique to simplify the routing table is called the Next-hop method.

→ Routing table holds only address of the next hop.

2. Network-Specific Method:

→ This technique helps to reduce the routing table and simplify the searching process.

→ Here, we have only one entry that defines the address of the distination network itself

3. Default Method:

→ Another technique to simplify routing is called the default method.

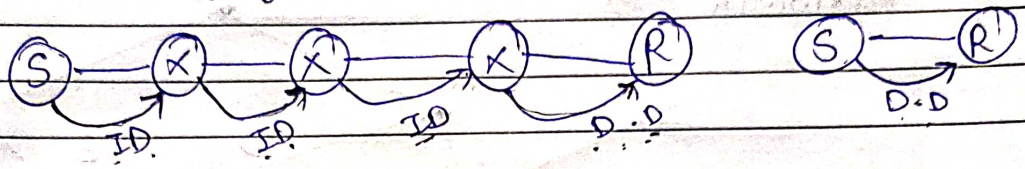
→ In this technique instead of listing all networks in the entire Internet, host just has one entry called the default.

→ It is normally defined as network address 0.0.0.0

Page No.:
Date: / /

Delivery

→ Delivery refers to the way a packet is handled by the network layer.
→ The network layer supervises the handling of the packets by the underlying physical networks.



1. Direct Delivery

→ Packet reaches final destination
→ via router or Sender itself

2. InDirect Delivery

→ Packet reaches intermediate node & not final destination
→ via router or Sender itself.

Routing Algorithms

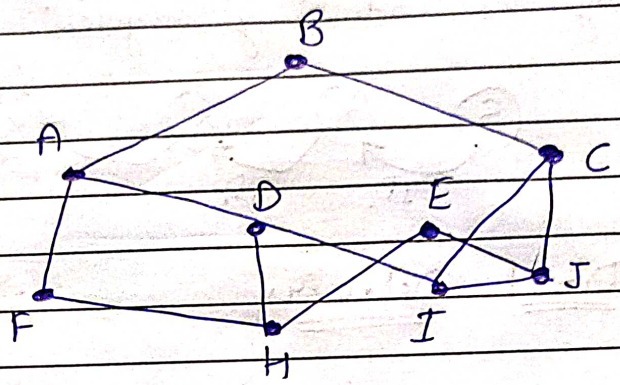
Static	Dynamic
→ Shortest path Routing	→ Distance Vector Routing
→ Flooding	→ Link State Routing
→ Flow Base Routing	

Page No.
Date / /

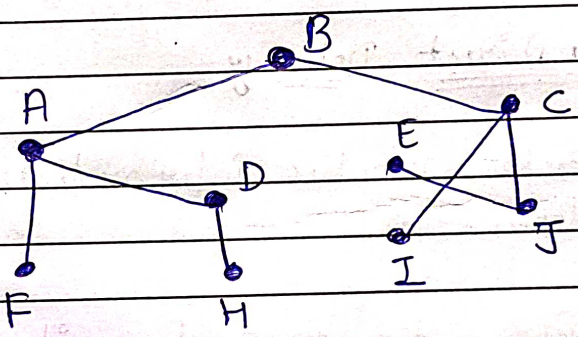
1. The Optimality Principle:

Each portion of a best path is also a best path; the union of them to a router is a tree called the sink tree.

Network ⇒



Sink tree of best paths to router B ⇒



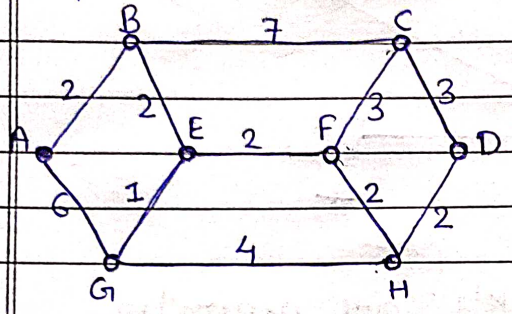
2. Shortest Path Algorithm

a) Dijkstra's algorithm computes a sink tree on the graph.
b) Each link is assigned a non-negative weight / distance.

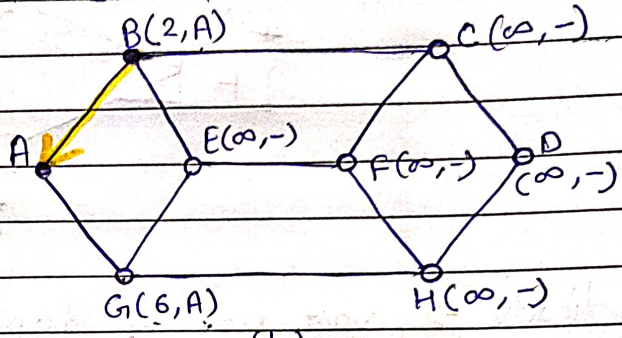
Page No.:
Date:

Algo:

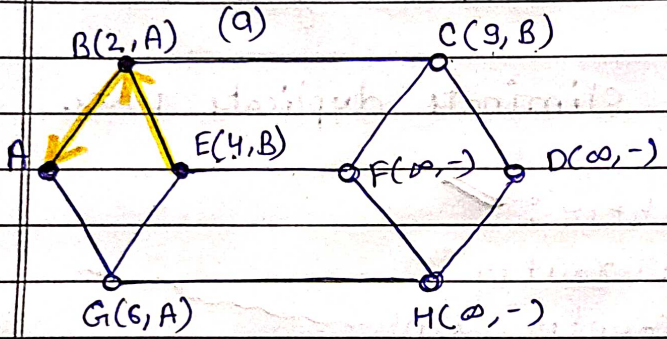
a) Start with sink, set distance at other nodes to infinity.
b) Relax distance to adjacent nodes
c) Pick the lowest adjacent distance node, add it to sink tree.
d) Repeat untill all nodes are in the sink tree.



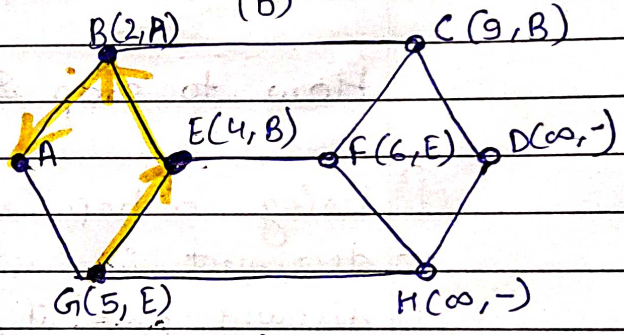
(a)



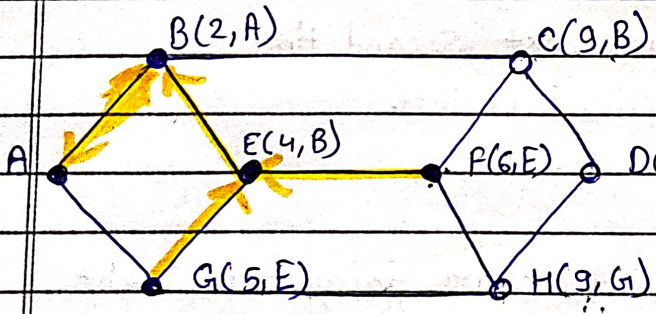
(b)



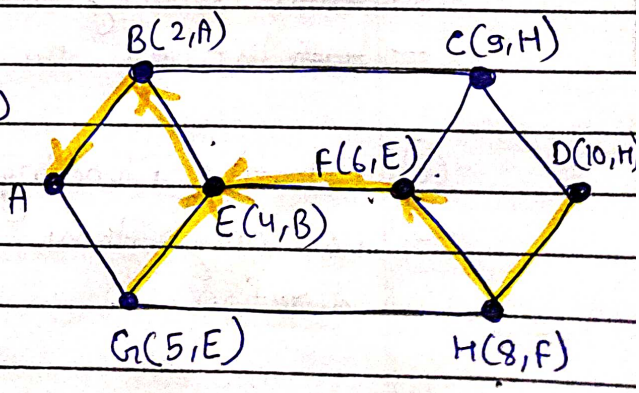
(c)



(d)



(e)

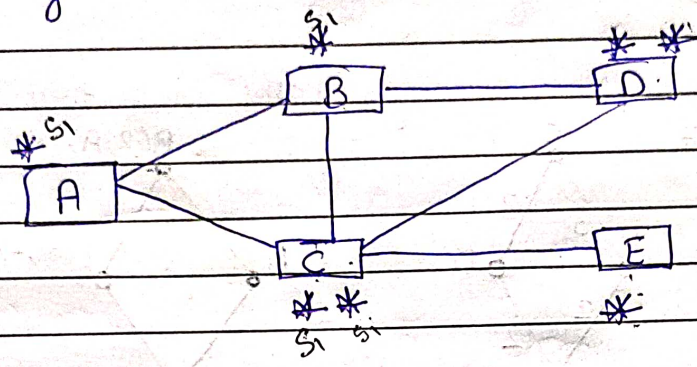


(f)

Page No.
Date: /

3. Flooding

→ A simple local technique is Flooding, in which every incoming packet is sent out on every outgoing line except the one it arrived on.



disadv → vast no. of duplicate pkts are generated.

How to stop & Eliminate duplicate pkts.

① Using a hop counter:
- decrement in each router
- discard pkt if counter is '0'

② Sequence no. in pkt:
- avoid sending the same pkt second time
- ~~lists~~ list all the received packets.

③ Selective Flooding:
- use only those lines that are going in right direction.

Page No.:
Date:

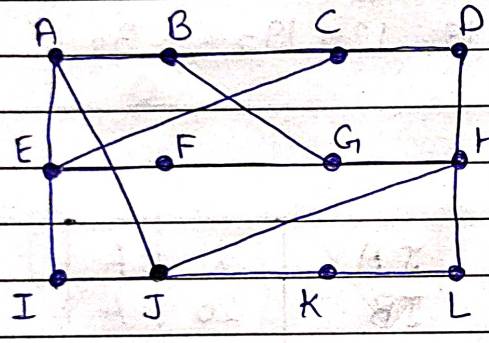
AKTU - 2021-22 [10 marks].

4. Distance Vector Routing

→ It is an Unicast Routing Protocol.
→ DVR uses the Bellman-Ford algorithm.

Algo:-
a) Each node knows distance of links to its neighbours.
b) Each node advertises vector of lowest known distances to all neighbours
c) Each node uses received vectors to update its own.
d) Repeat periodically.

e.g.→



To	A	I	H	K
A	0	24	20	21
B	12	36	31	28
C	25	18	19	36
D	40	27	8	24
E	14	7	30	22
F	23	20	19	40
G	18	31	06	31
H	17	20	0	19
I	21	0	14	22
J	9	11	7	10
K	24	22	22	0
L	29	33	9	9
	JA	JI	JH	JK
	delay	delay	delay	delay
	8	10	12	6

→ We have to find New estimated delay from J.

Page No.
Date / /

→ JA → min (JA + AA, JI + IA, JH + HA, JK + KA)

min (8 + 0, 10 + 24, 12 + 20, 6 + 21)
(8, A)

→ JB → min (JA + AB, JI + IB, JH + HB, JK + KB)

min (8 + 12, 10 + 36, 12 + 31, 6 + 28)
(20, A).

→ JC → min (JA + AC, JI + IC, JH + HC, JK + KC).

min (8 + 25, 10 + 18, 12 + 19, 6 + 36).
(28, I).

JA	8	A
JB	20	A
JC	28	I
JD	20	H
⇒ JE	17	I
J	30	I
'	18	H
'	12	H
'	10	I
'	0	-
	6	K
JL	15	K

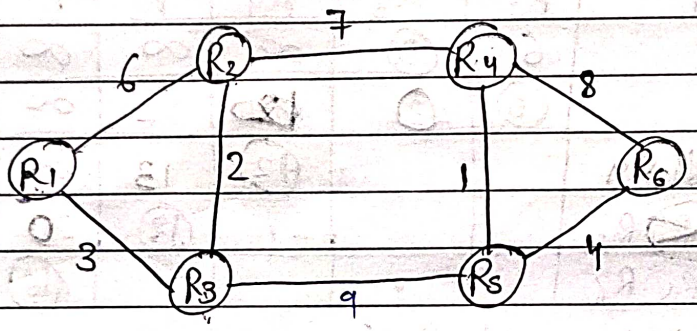
New vector for J

Page No.:
Date: / /

5. Link State Routing

→ It is an Unicast Routing Protocol.
→ Discover its neighbours and learn their network addresses.
→ Set the distance metrics to each of its neighbours.
→ Construct a packet telling all it has just learned.
→ Computs the shortest path to every other router.
→ Using this packet (send this packet to and receive packets from all other routers).

Eg⇒



Table

1st ⇒

R1	
Seq. No.	
111	
R2	6
R3	3

R2	
R1	6
R3	2
R4	7

R3	
R1	3
R2	2
R5	9

R4	
R2	7
R5	1
R6	8

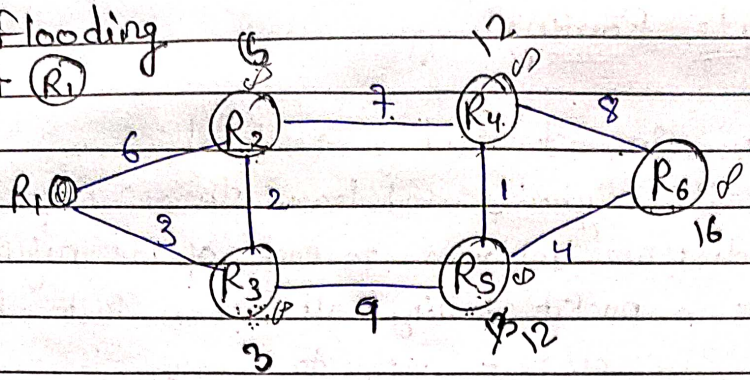
R5	
R3	9
R4	1
R6	4

R6	
R5	4
R4	8

Step 1

Page No.
Date / /

2nd Flooding at R_1



3rd Dijkastra.

R_1	R_2	R_3	R_4	R_5	R_6
$R_1 R_3$	6	(3)	∞	∞	∞
$R_1 R_3 R_2$	(5)	(3)	~~∞~~	12	∞
$R_1 R_3 R_2$ ~~R_4~~ R_4			(12)	13	∞
$R_1 R_3$ ~~$(R_2 \; R_4)$~~ R_5				(13)	20
$R_1 R_3 R_5$ R_6					(16)

4th Routing Table of R_1

		Via
R_1	0	R_1
R_2	5	R_3
R_3	3	R_1
R_4	12	$R_3 R_2$
R_5	12	R_3
R_6	16	$R_3 R_5$

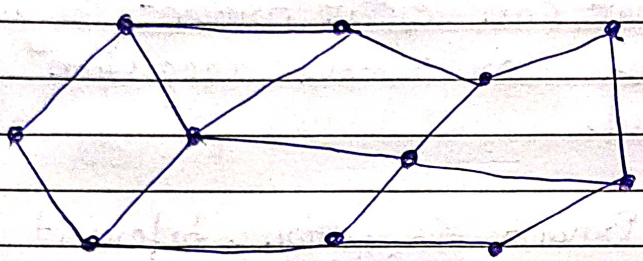
AKTU - 2018-19 Q→ Unicast Routing Protocols.
1. – DVR
2. – Link state Routing

Page No.:
Date : / /

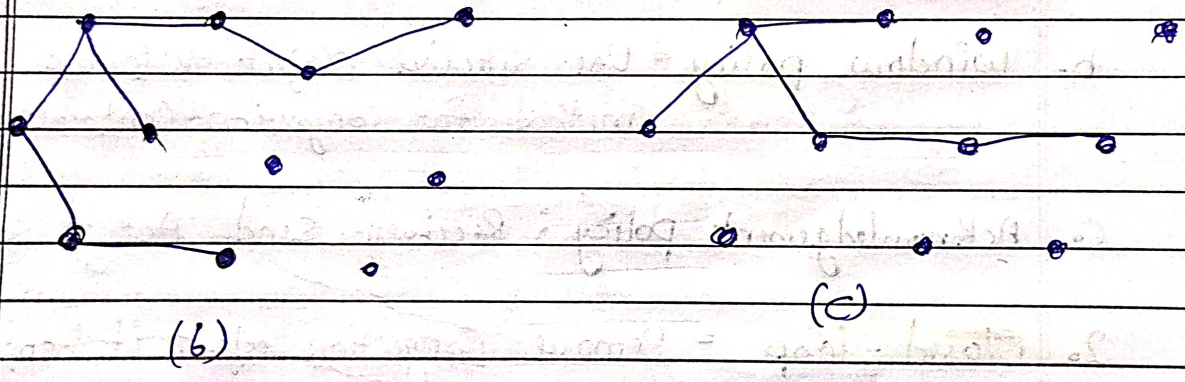
6. Multicast Routing

→ Sending a massage to a group is called multicasting. Multicasting requires group management need to create & destroy groups. For multicast routing each router computes a spanning tree covering all other routers.

e.g.



(a) network.



(b) (c)

7. Broadcast Routing

→ Sending a packet to all destinations simultaneously is called broad casting.

1. Multi destination Routing.
2. Flooding
3. Sink tree.

Page No.
Date: / /

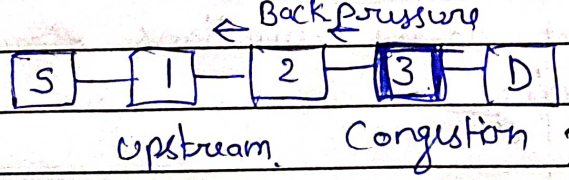
DKTU 2017-18 [10 marks]

Congestion

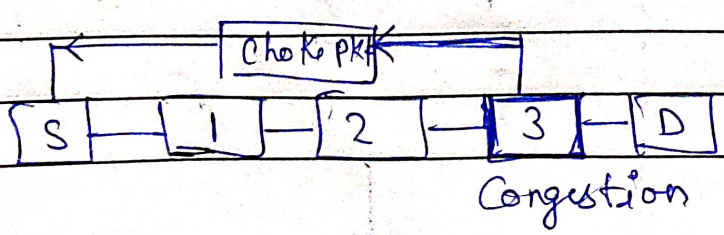
→ Congestion in a network may occur if the load on the network is greater than capacity of network.

Congestion Control : It refers to techniques and mechanisms that can either prevent congestion, before it happens or remove congestion, after it has happened.

1. **Open Loop** = Prevent Congestion, before it happens)
   a. Retransmission policy = pkt can be retransmitted
   b. Window policy = Use Selective reject window method for Congestion Control
   c. Acknowledgement policy : Reciver send Ack to Sender
2. **Closed - loop** = Remove Congestion after it happens.
   a. Back pressure = In this congested node stops receiving data from the immediate upstream nodes.



   b. Choke packet =



Page No.:
Date:

c. Implicit signaling = there is no communication b/w congested node or node and the source.

→ Source guesses there is a congestion in network. when it does not receive any ack.

d. Explicit signaling = sending direct signal to source or destination.

Quality of Service (QoS) AKTU-2018-19 [10 marks]

→ QoS is an overall performance measure of computer Network.

(1) Reliability ⇒ lack of Reliability means loosing Packet or Acknowledgement, which result Retransmission.
e.g → Email, File Transfer, Internet Access (More Reliability Need)

(2) Delay ⇒ It is time taken to transmit Packet from source to Destination in flow.

(3) Jitter ⇒ Jitter is variation in Packet Delay.

(4) Bandwidth ⇒ It is number of bit send.

Page No.
Date: / /

QoS Table

Application	Bandwidth	Delay	Jitter	Loss
Email	Low	Low	Low	Medium
File sharing	High	Low	Low	Medium
Web access	Medium	Medium	Low	Medium
Remote login	Low	Medium	Medium	Medium
Audio	Low	Low	High	Low
Video	High	Low	High	Low
Telephony	Low	High	High	Low
Video conferencing	High	High	High	Low

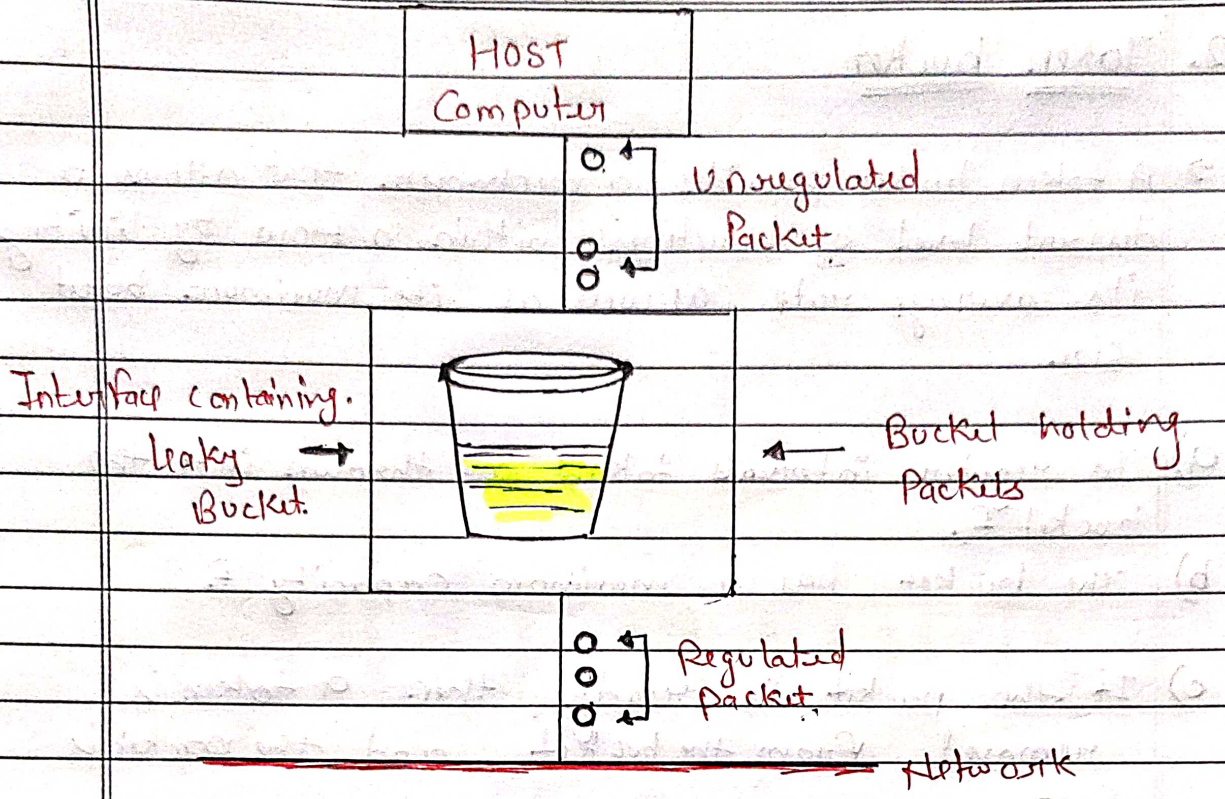
Congestion Control Algorithms:

1. Leaky Bucket

The Leaky Bucket Algorithm is a method of congestion control where multiple packets are stored temporarily. These packets are sent to the network at a constant rate. This algo is used to implement congestion control through traffic shaping in data networks.

→ a bit overdone and also packet can get lost (bucket is full)

Page No.:
Date:



Step1 ⇒ Initialize buffer size & leak rate.

Step2 ⇒ At clock tick, Initialize n as the leak rate.

Step3 ⇒ If n > size of packet (Send the packet into N/w)
(n − size of Pa)

Step4 ⇒ Decrement n by the size of the packet

Step5 ⇒ Repeat step 3 and step 4 untill n < size of pkt
No other packet can be transmitted till the next clock tick

Step6 ⇒ ~~Go~~ Go to Step2.

Page No.
Date / /

2. Token bucket

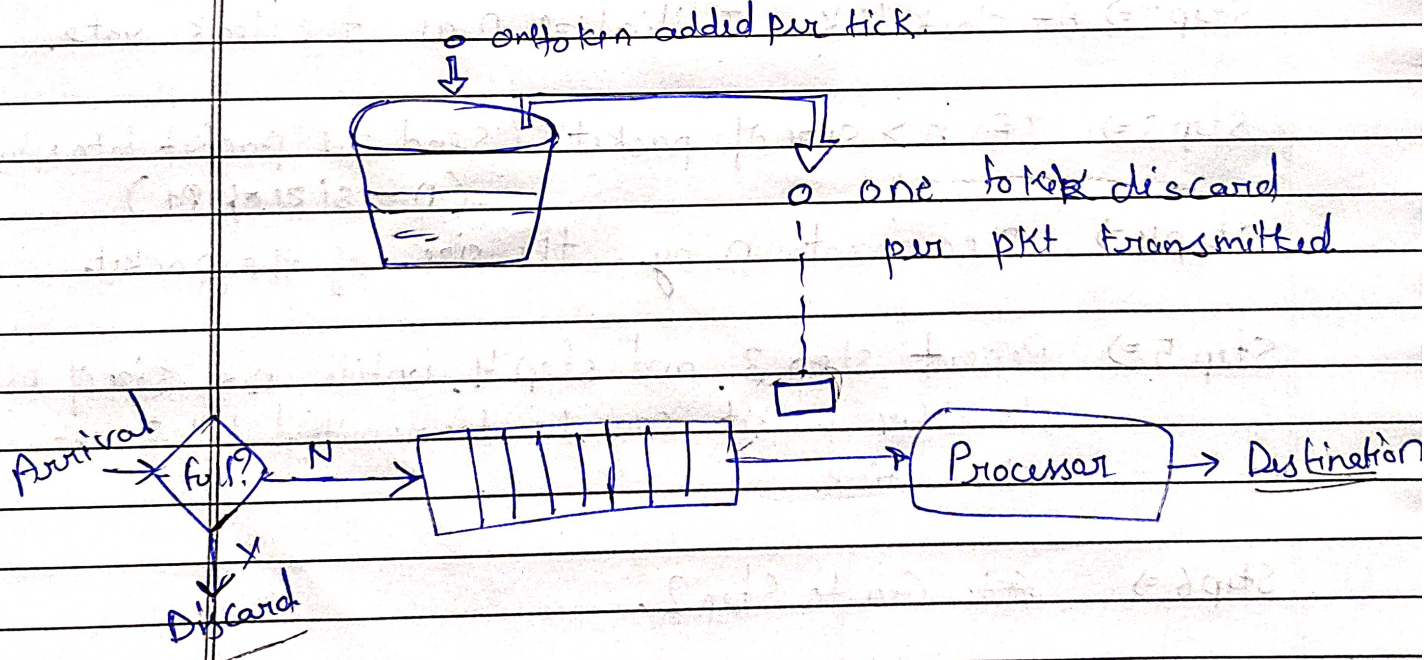
⇒ A token bucket provides a mechanism that allows a desired level of burstiness within a flow by limiting its average rate as well as its maximum burst size.

a) In regular intervals tokens are thrown into the bucket f.

b) The bucket has a maximum capacity f.

c) If the packet is ready, then a token is removed from the bucket, and the packet is sent

d) Suppose, if there is no token in the bucket, the packet cannot be sent.



Page No.:
Date:

Unit-3 Completed