Network Layer:

→ The network layer is responsible for carrying the Packet from the source all the way to destination. In short it is responsible for host-to host delivery.

→ The network Layer has a higher responsibility than the DLL. because the DLL is only supposed to move the frames from one end of the wire to the other end.

→ Thus network layer deals with the end to end transmission.

Position of Network Layer:- The position of Network are as follows:

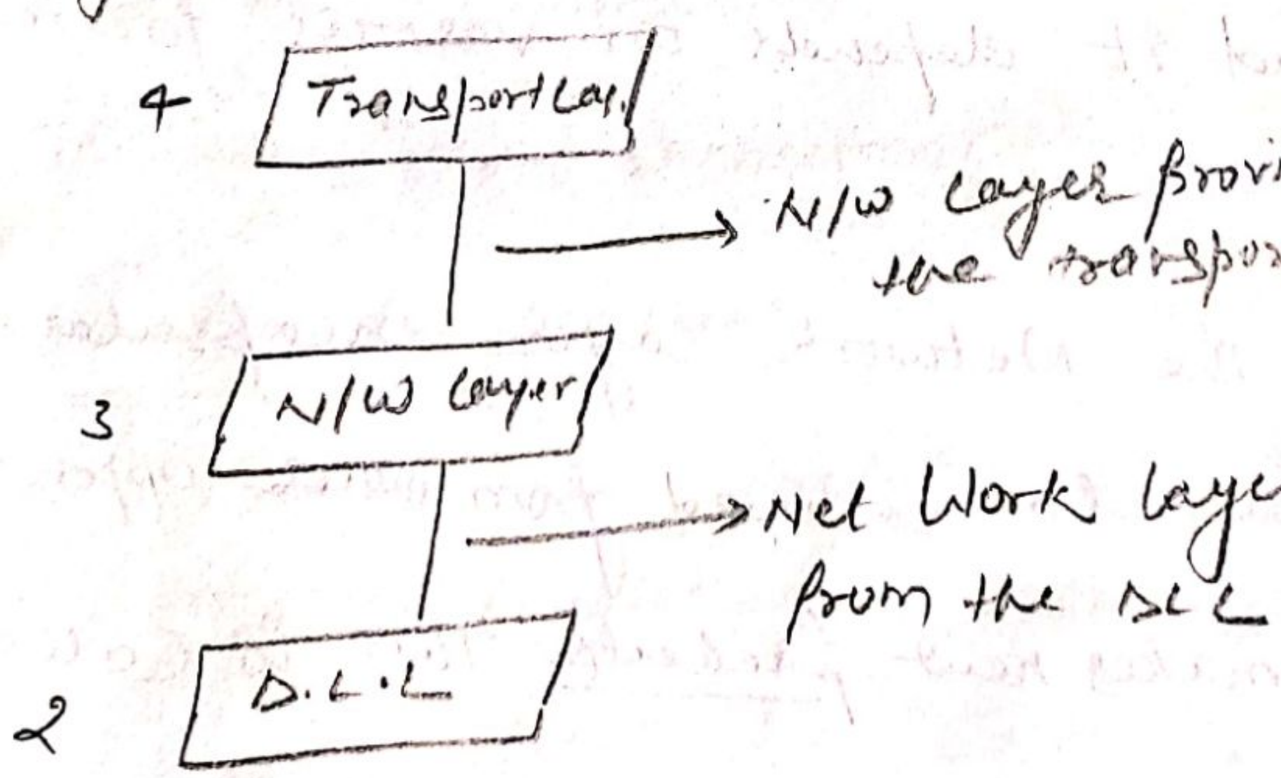


fig: Position of Network Layer

Responsibilities or duties as functionality

Duties of Network Layer: Are as follows:

① **Interneworking**: This is the main duty of Network Layer. (It provides the logical Connection between different types of Networks.)

② **Addressing**: Addressing is necessary to identify each device on the internet uniquely. This is similar to a telephone System. The address used in the network layer should uniquely and universally define the connection of a computer.

③ **Routing**: In a Network, there are multiple routes available from a source to a destination and one of them is to be choosen (selected) (taken). The Network layer decides the route to be taken. This is called as routing and it depends on various factors.

④ **Packetizing**: The Network layer encapsulates the packets received from other upper layer protocol and makes new packets. This is called as packetizing. It is done by the a Network layer protocol called IP (Internetworking protocol).

Scanned with OKEN Scanner

(iv) Fragmenting: The datagram can travel through different networks. Each router decapsulates the IP datagram from the received frame. Then the datagram is processed and encapsulated in another frame.

Network layer services: (Two types of services provided by n/w lay.)

(i) Connection-oriented services
(ii) Connection-less services

(i) Connection oriented services:

→ The connection oriented service is similar to, for example "Telephone System services", or virtual circuit,
→ The service users of the connection oriented service is follow the several operation.

(a) Establish a connection
(b) use the connection
(c) Release the connection.

(ii) Connection less service:

→ This is like the Postal service, "datagram".
→ Each message (analogus to a letter) carries the full address of the destination. Each message is routed independently from source to destination through the system.
→ It is possible that the order in which the message are sent and the order in which they are received may be different.

Scanned with OKEN Scanner

Virtual circuits:

→ The principle behind the virtual circuits is to choose only one route for from source to destination.

→ When a connection is established, it is used for all the traffic flowing (same root) over the connection.

→ When the connection is released, the virtual circuit is terminated.)

Features of virtual circuits:-

→ In virtual circuits every router has to maintain a table.

→ Each packet must have a virtual circuit number field in its header in addition to sequence number, checksum etc.

→ Circuit set up is required in virtual circuits. The virtual circuits can be initiated from either end. But problem can arise if call set ups are propagating in both directions simultaniously.)

arise

Scanned with OKEN Scanner

Internetworking devices or Network Connecting device: Are as follows.

1. Repeater
2. HUB
3. Bridges
4. Switches
5. Routers
6. Gateways

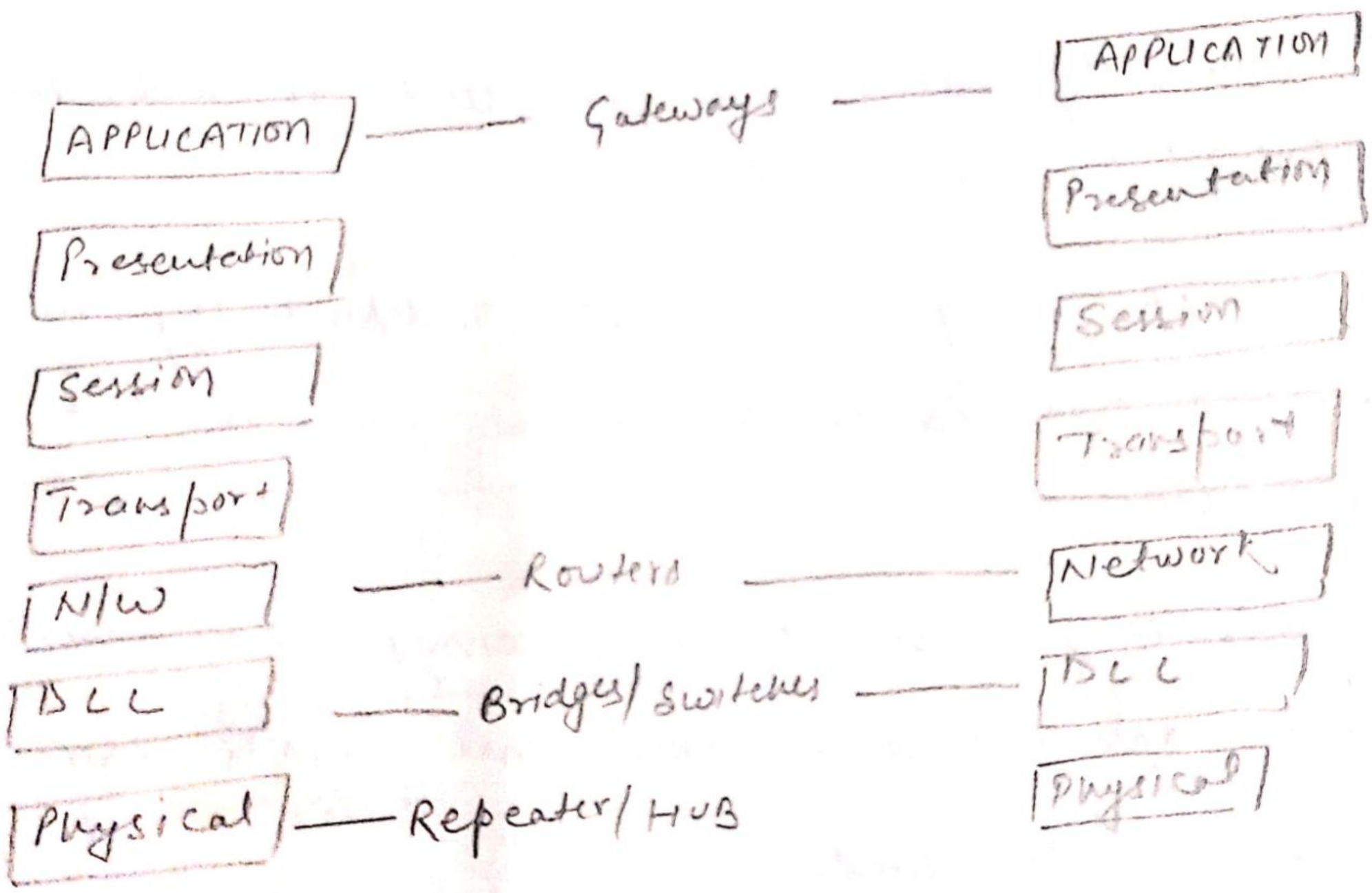


fig: Internetworking device or Connecting device

Internet Protocal (IP):

→ This is the host to host network layer delivery protocal designed for the Internet.

→ IP is a connectionless datagram protocal with no ~~guar~~ guarantee of reliability.

→ It is a unreliable protocal (because it does not provide any error control or flow control.

→ IP can only detect the error and discards the packet if it is corrupted.

→ Each IP datagram is handled independently and each one can follow a different route to the destination.)

→ So there is a possibility of receiving out of order packets at the destination. Some packets may even be lost or corrupted.

→ IP relies on a higher level protocal to take care of all these problems.

Datagram: (IP transports data in packets called datagrams, each of them ~~which~~ is transported separately. Datagram may travel along different routes and may arrive out of sequence or duplicated. IP does not keep track of the routes and has no facility for reordering

datagrams once they arrive. Because its a connection less service. IP does not create virtual circuits for delivery.

→ (A data gram is a variable length packet with two parts : Header and data. (up to 65536 bytes). The header can be from 20 to 60 bytes and contains information essential to routing and delivery.)

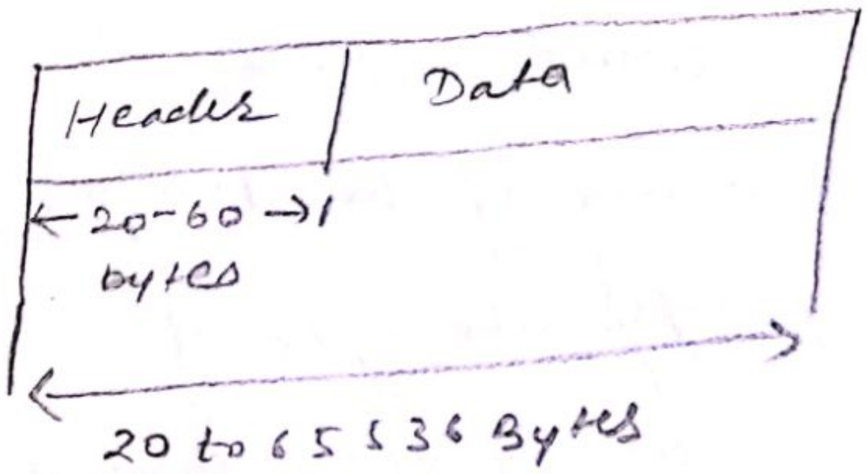


fig IP data gram format

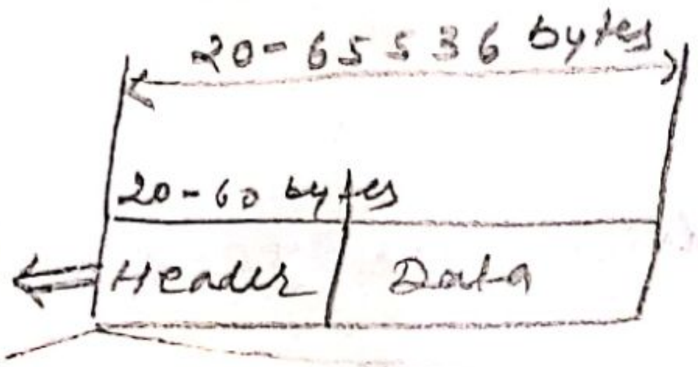
Structure of IP frame Header :- OR IP datagram

The IP frame header contains routing information and control information associated with ~~dog~~ datagram delivery. TCP/IP to show the header in four bytes (32 bits) sections. The brief description of each field is in or are as follows:)

1. ver (version): This field define the version of IP. The current version is 4 (IPv4) with a binary value of 0100.

(2) Header length (HLEN): The HLEN field defines the length of the header in multiples of four bytes. The four bits can represent a number between 0 and 15, which, when multiplied by 4, gives a maximum of 60 bytes. (The maximum value of this 4 bit field is 15 which limit the header to 60 Bytes, & thus the options field to 40 Bytes)

(iii) Service type: This service type field defines how the datagram should be handled. It includes bits that define the priority of the datagram. It also contain bits that specify the type of service the sender desires. such as the level of throughput, reliablity and delay



32
8

VER 4 bits	HLEN 4 bits	Service ~~Byte~~ type 8 bits	Total length 16 bits
Identification 16 bits		Flags 3 bits	Fragementation offset 13 bits
Time to live 8 bits	Protocols 8 bits	Header check sum 16 bits	
Source IP address 32 bits			
Destination IP address 32 bits			
Option			

32×5
= 160 bit / 8
= 20 Byte

fig IP Frame Header or IP datagram

(iv) Total length: The total length field defines the total length of the IP datagram. It is a two byte field (16 bits) and can define up to 65535 bytes ($2^{16}-1$).

(v) Identification: The identification field is used in fragmentation. A datagram, when passing through different networks, may be divided into fragments to match the network frame size. each fragement is identified with a sequence number in this field.

(vi) Flags: There bits in the flags field deal with fragmentation. (the datagram can or cannot be fragmented, / can be the first, middle or last fragement etc.)).

(vii) Fragmentation offset: The fragmentation offset is a pointer that shows the offset of the data in the original datagram. if it is fragmented

(viii) Time to live: The time to live field defines the number of hops a datagram can travel before it is discarded.

Scanned with OKEN Scanner

(ix) Protocal: The protocal field defines which upper layer protocal data are encapsulated in the datagram. (TCP, UDP, ICMP etc)
(Internet control message protocal)

(x) Header Checksum: This is a 16 bit field used to check the integrity of the header, not the rest of the packet.

(xi) Source address: The source address field is a four byte (32 bits) Internet address. It identifies the original source of the datagram.

(xii) Destination address: The destination address field is a four byte (32-bits) Internet address. It identifies the final destination of the datagram.

(xiii) Options: The options field gives more functionality to the IP datagram. It can carry fields that control routing, timing, and management.

Scanned with OKEN Scanner

IP Addresses: [Each internet address consists of four bytes (32 bits), define three fields: Class type, net id, and Host id.] These parts are of varying lengths, depending on the class of the address.

An Internet address is made of four bytes (32 bits), that define a host connection to a N/W

fig Internet address

→ Every host and router on the Internet has a unique IP address.

→ All the IP addresses are 32 bit long and they are used in the source address and destination address fields of the IP header.

→ The IP number (addresses) for the hosts are assigned by the Network administrator. for a public network on the Internet, we have to obtain a network number assigned by the network Information center.

⇒ IP address consists of two parts. The first parts of the address, called the Network number, identifies a network on the Internet, and second

(ix) Protocol.

the host id, identifies an individual host on the network.

	Byte 1	Byte 2	Byte 3	Byte 4
C class	0 Net id		Host id	
class B	10 Net id		Host id	
class C	110 Net id			Host id
class D	1110 Multi cast addresses			
class E	1111 Reserved for Future use			

A- 00000000 - 01111111
B- 10000000 10111111
C - 11000000 - 11011111
D- 11100000 - 11101111
E- 11110000 - From 11111111

fig Internet classes

Class A 0.0.0.0 (Net id, Host id) → 127.255.255.255 (Net id, Host id)

Class B 128.0.0.0 (Net id, Host id) — 191.255.255.255 (Net id, Host id)

Class C 192.0.0.0 (Net id, Host id) — 223.255.255.255 (Net id, Host id)

Class D 224.0.0.0 (Group address) — 239.255.255.255 (Group address)

Class E 240.0.0.0 (undefine) — 255.255.255.255 (undefined)

fig class ranges of Internet address

Decimal Notation: To make the 32-bit form shorter and easier to read, internet address are usually written in decimal form with decimal point separating the bytes - Decimal notation.

Sep

128	11	3	31
10000000	00001011	00000011	00011111

(If address in decimal notation)

Class A address:

→ The network field is 7 bit long and the host field is of 24 bits length.

→ The host numbers will range from 0.0.0.0 to 127.255.255.255

→ Class A, there can be 126 types of Network and 17 Millions host.

→ The '0' in the first field identifies that it is a class A network address.

Class B: → The first two fields identify the network and the number in the first field must be in the range 128-191.

→ Class B Network are large. Host numbers 0.0 and 255.255 are reserved, so there can be upto 65534 $(2^{16}-2)$ ~~host~~ in a class B Network.

$(2^{16}-2)$ $(256 \times 256)-2$ $65536-2=65534$

→ The first block covers address from 128.0.0.0 to 128.255.255.255. and the last block covers from 191.255.0.0 to 191.255.255.255.

Class C:

→ The first block in class C covers address from 192.0.0.0 to 192.0.0.255 and the last block covers address from 223.255.255.0 to 223.255.255.255.

Class D:

→ The class ~~address~~ format allow for upto 2 million networks with up to 254 ~~(2^8~~ hosts each, and it's class D format allows the multicast in which a datagram is directed to multiple hosts.

Class E: — reserve for future use

→ The 32 bit (4 byte) network address are usually written in ~~dott~~ decimal notation. In this notation each of the 4 bytes is written in decimal from 0 to 255.

→ So the lowest IP address is 0.0.0.0 i.e. all the 32 bit are zero and the highest IP address is 255.255.255.255.

Scanned with OKEN Scanner

Examples: What is the class of each of the following addresses?

(a) 10011101 10001111 11111100 11001111

(b) 11011101 10001111 11111100 11001111

(c) 01111011 10001111 11111100 11001111

(d) 11101011 10001111 11111100 11001111

(e) 11110101 10001111 11111100 11001111

128 16 8 4 1 = 157

128 8 15 = 143

4 16 32 64 128 = 252

128 64 15 = 207

= 157.143.252.207

Sol:
(a) Class B
(b) Class C
(c) Class A
(d) Class D
(e) Class E

Numerical 2: For the address 24.46.8.95 identify the type of network and find the network address.

Sol^n:

→ Examine the first Byte 24 i.e. it is between 0 and 127, so it is a call class A network.

→ We know that in class A have only first byte defines the Netid. So we can find the network address by replacing the host id with 0's.

→ The Process of obtain the Network address is:

$\boxed{24.46.8.95}$

Netid ↓ hostid

replace hostid by 0's

⇒ $\boxed{24.0.0.0}$ → Network address.

Scanned with OKEN Scanner

Num. 3: For the address 132.7.21.84 find the type of Network and the Network address.

Sol^n: examine the first byte. It is 132 ie between 128 and 192 so it is a Class B Network.

. So the first two Byte define the Net id. Replace the hostid with 0's to get the Network address.

132. 7. 21. 84
Netid Hostid

↓ Hostid replace by 0's

132.7.0.0 ⇒ Network address.

Q-4: Find the class of the Network if the address is 221.46.75.64. & Network address.

Sol^n: The first byte is 221 i.e. between 192 and 223 so this is a Class C Network.

- In class C, First 3 byte is Netid and last byte is Hostid.

221.46. 75.64
Netid hostid

change is 0's

⇓

= 221.46.75.0 Network address.

Scanned with OKEN Scanner

Note:

The Network address is different from a Net id. A Network address has both netid and host id. with 0's for host id.

The Net work address is used to route the packets to the desired location.)

IPV6: (IPV6 is the next generation Internet Protocol designed as a successor to the IP version 4.

IPV6 was designed to enable high performance, scalable Internet). This was achieved by over coming many of the weakness es of IPV4 protocol and by adding several New features.)

Advantages of IPV6:

1. Larger address space: IPV6 has 128-bit address space which is 4 times (largus) wider in bits in compared to IPV4's (32 bit) address space. So there is a large (wide, huge) increase in the address space.

2. Better header format:

→ IPV6 uses a better header format, In its header format the options are separated from the base header.

Scanned with OKEN Scanner

③ New options: New options have been added in IPV6 to increase the functionality. The options are inserted when needed, between the base header and upper layer data. It helps in speeding up the routing process.

④ Possibility of extension: IPV6 has been designed in such a way that there is a possibility of extension of protocol if required.

⑤ More Security: IPV6 includes security in the basic specification. It includes encryption of packets (ESP: encapsulated security payload) and authentication of the sender of packets. (AH. Authentication Header).

⑥ Support to Resource allocation: To implement better support for real time traffic (such as video conference), IPV6 includes flow label in the specification. With flow label mechanism, routers can recognize to which end to end flow the packets belongs.

Scanned with OKEN Scanner

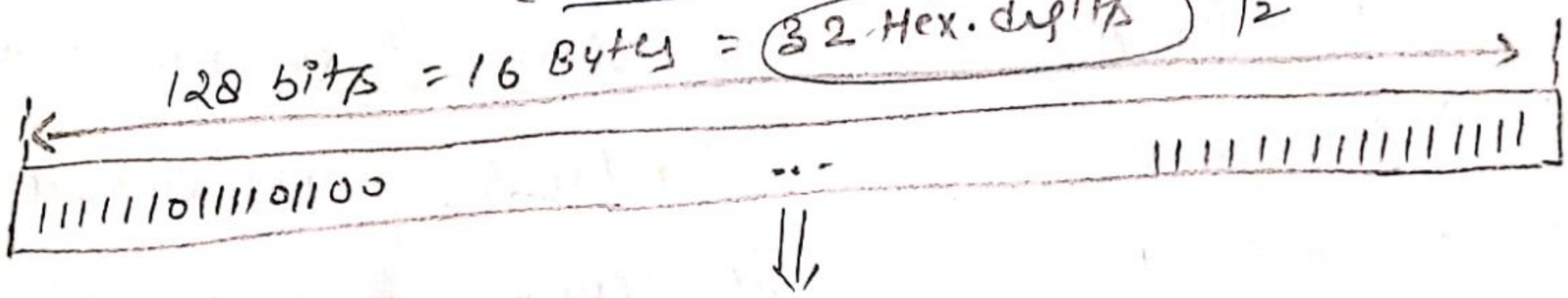
7. Plug and Play: IPV6 includes plug and play in the standard specification. It these force must be easier for novice (beginner (new)) users to connect their machines to the Network, it will be done automatically.

8. Clearer Specification and optimization: IPV6 follows good practices of IPV4, and reject minor flaws (defect) / obsolete (disused, no longer used) items of IPV4.

IPV6 Addresses:

[16 bits = 4 Hex. digits
128 " = 32 Hex. digit]

128 bits = 16 Bytes = 32 Hex. digits $\times 4 = 128$ bit



FDEC : BA98 : 7654 3210 : ADBF : BBFF : 2922 : FFFF

Hexadecimal Colon Nation :- To make address more readable, IPV6 specifies hexadecimal Colon notion. In this notation, 128 bits are divided into eight sections, each 2 bytes in length. Two bytes in hexadecimal notation requires four hexadecimal digits. Therefore, the address consists of 32 hexadecimal digit, with every 4 digits seperated by a Colon.)

Assignment 4

① Explain the different types of routing algorithm

Static

1. ① Shortest path alg.
2. ② Flooding
3. ③ Flow based routing

Dynamic

1. ① Distance vector Routing
2. ② Count to infinity Problem
3. ③ Link state Routing
4. ④ Hierarchical Routing
5. ⑤ Routing for Mobile host

Q Find the class of each address & Network address.

Sol
ⓐ 4.23.145.90
ⓑ 227.34.78.7
ⓒ 246.7.3.8
ⓓ 29.6.8.4
ⓔ 198.76.9.23

→ Sol:
ⓐ Class A, Network address 4.0.0.0
ⓑ Class D, No Network address
ⓒ Class E, No Network address
ⓓ Class A, Network address 29.0.0.0
ⓔ Class C, " " 198.76.9.0

Q Find the Network address for each address, & class and Netid, Hostid.

Sol ⓐ 4.23.145.90

Sol Class A, Network address = 4.0.0.0, Netid 4, hostid 23.145.90

ⓑ 227.34.78.7

Sol Class D, No Netnetwork address, No Netid, No hostid

ⓒ 246.7.3.8

Sol Class E, No Network address, No Netid, No hostid

ⓓ 129.6.8.4

Sol Class B, Network address = 129.6.0.0, Net id = 129.6, Hostid 8.4

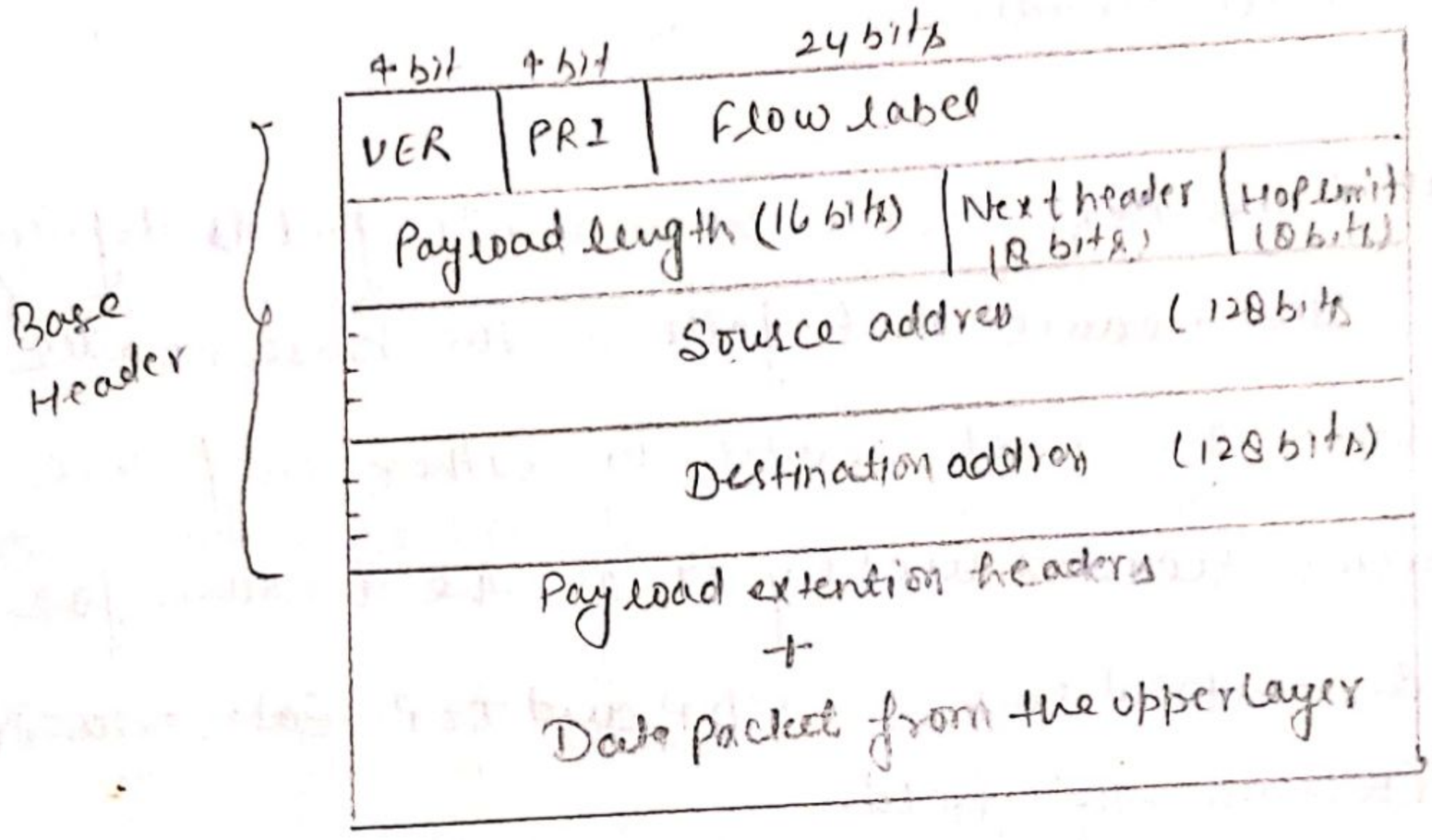
ⓔ 198.76.9.23

Sol Class C, Network address = 198.76.9.0, Netid = 198.76.9, Hostid = 23

Scanned with OKEN Scanner

Imp 1 ~~ah~~ 5c

IPV6 Packet Format: Each packet is composed of a mandatory base header followed by the payload. The Payload consists of two parts: optional ~~extentio~~ extension headers and data from an upper layer. (The Base header occupies 40 bytes, whereas the extension headers and data from the upper layer contain up to 65,535 Bytes of Infor.)



=> 32 bits = 4 byte
=> 32 " = 4 byte
= 128 " = 16 byte
= 128 " = 16 byte
Base Header = 40 Byte

fig: Format of an IPV6 datagram

Base Header: Base Header having eight fields. These fields are as follows:

(i) **version:** This 4 bit field defines the version number of the IP. for IPV6, the value is 6. $(0110)_2$

(ii) **Priority:** The four (4) bit priority field defines the priority of the packet with respect to traffic congestion.

(iii) Flow label: The flow label is a 3-byte (24 bits) field that is design to provide special handling for a particular flow of data.

(iv) Payload length: This 2-byte payload length field defines the total length of the IP datagram excluding the base header.

(v) Next header:- The next header is an 8 bit fields defining the header that follows the base header in the datagram. The next header is either one of the optimal extension headers used by IP or the header for an upper layer protocol such as UDP and TCP. Each extension header also contains this field.

(vi) Hop limit: This 8 bits hop limit field server the same purpose as the TTL (Time to live) field in IPV4.

(vii) Source address: The source address field is a 16 byte (128 bits) internet address that identifies the original source of the datagram.

(viii) Destination address: This ~~ade~~ The destination address field is a 16 byte (128-bits); Internet address that usually identifies the final destination

Scanned with OKEN Scanner

of the datagram. However if, source routing is used, this field contains the address of the next router.

Extension Headers: (The length of the Base header is fixed at 40 Bytes.) However, to give of more functionality to IP datagram, the Base header can be followed by up to six extension headers, many of these headers are options in IPV4.

Imp

Unicast, Multicast and Broadcast addresses: Communication on the Internet can be achieved using unicast, multicast or broadcast addresses.

(1) **unicast address:** Unicast address is one-to-one. When a packet is sent from an individual source to an individual destination, a unicast communication take place. All systems on the Internet should have at least one unique unicast address. unicast address belong to class A, B, or C.

(2) **Multicast address:** Multicast communication is one-to many. when a packet is sent from an individual source to a group of destinations, a multicast communication has taken place. A multicast address is a class D address. The whole address define a group id. Multicasting on the Internet can be on the local level or global level. At the local level, hosts on a LAN can form a

group and be assigned a multicast address. At the global level, hosts on different networks can form a group and be assigned a multicast address.

③ Broadcast addresses: Broadcast communication is one-to-all. The Internet allows broadcasting only at the local level. No broadcasting is allowed at the global level. This means that a system (host or router) cannot send a message to be received by all hosts and routers in the Internet. One of the reasons for this restriction is to prevent a huge traffic jam.

A - 10.0.0.0 — 10.255.255.255 (16,777,216 Host) = 256 × 256 × 256
B - 172.16.0.0 - 172.31.255.255 (1,048,576 Host)
C - 192.168.0.0 - 192.168.255.255 (65536) Host

Private Networks: The Internet authorities have reserved three blocks of addresses.

B - (16 × 256 × 256) =
C - (256 × 256)

Class	Net id's	Total
A	10.0.0.0 - to 10.255.255.255	1
B	172.16.0.0 to 172.31.255.255	16
C	192.168.0.0 to 192.168.255.255	256

Host
- 16777216 Host (256×256×256)
1048576 " (16×256×256)
65536 " (256×256)

fig: Address of Private Network

Any organization can use an address out of this set without any permission from the Internet authorities. Everybody knows that these addresses are for private networks. They are unique inside the organization, but are not unique globally.

192.168.0.0 - 192.168.0.1
255 255

172.16.0.0 - 172.16.0.0
2 255
31 255

LALIT KUMAR

Routing Algorithm

Routers use **routing algorithms** to find the best route to a destination. When we say "best route," we consider parameters like the number of **hops** (the trip a packet takes from one router or intermediate point to another in the network), time delay and communication cost of packet transmission.

13 Oct

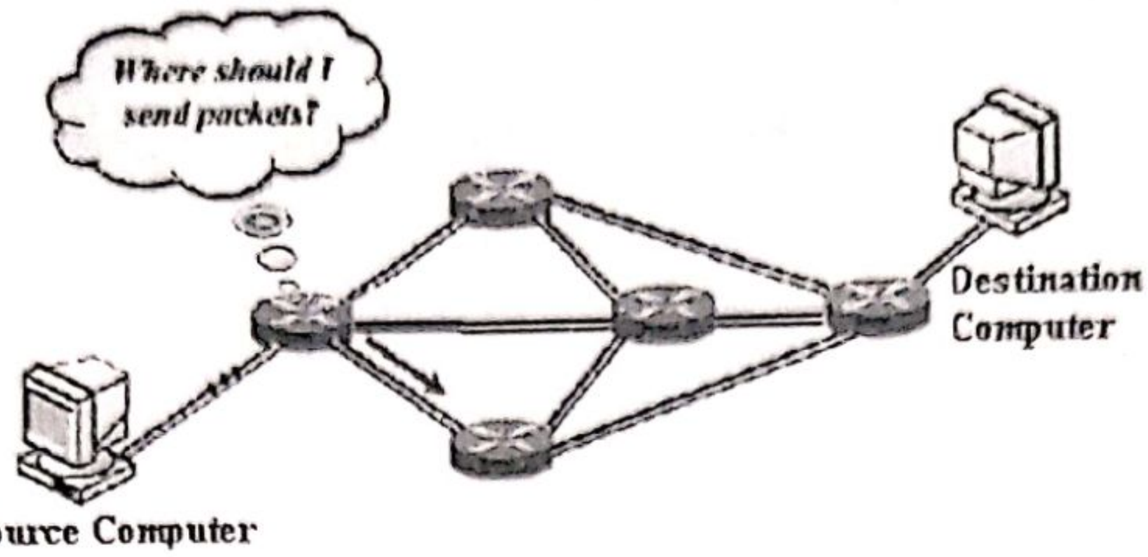


Fig: Packet Transmission from source to destination computer

Based on how routers gather information about the structure of a network and their analysis of information to specify the best route, we have two major routing algorithms: **global routing algorithms** and **decentralized routing algorithms**. In decentralized routing algorithms, each router has information about the routers it is directly connected to -- it doesn't know about every router in the network. These algorithms are also known as **DV** (distance vector) algorithms. In global routing algorithms, every router has complete information about all other routers in the network and the traffic status of the network. These algorithms are also known as **LS** (link state) algorithms.

Distance Vector Routing

In distance vector routing, each router periodically shares its knowledge about the entire network with its neighbors. There are three keys to understanding how this algorithm works are as follows:

- **Knowledge about the whole network-** Each router shares its knowledge about the entire network. It sends all of its collected knowledge about the network to its neighbors.
- **Routing only to neighbors-** Each router periodically sends its knowledge about the network only to those router to which it has direct links and used to update that router's own information about the network.
- **Information sharing at regular interval-** for example, every 30 seconds, each router sends its information about the whole network to its neighbors. This sharing occurs whether or not the network has changed since the last time information was exchanged.

Examine the internet shown in figure. In this example, the clouds represent local area networks. The number inside each cloud is that LANs network ID. These LANs can be of any type (Ethernet, Token ring, FDDI, etc). The LANs are connected by routers, represented by the boxes labeled A,B,C,D,E, and F.

Scanned with OKEN Scanner

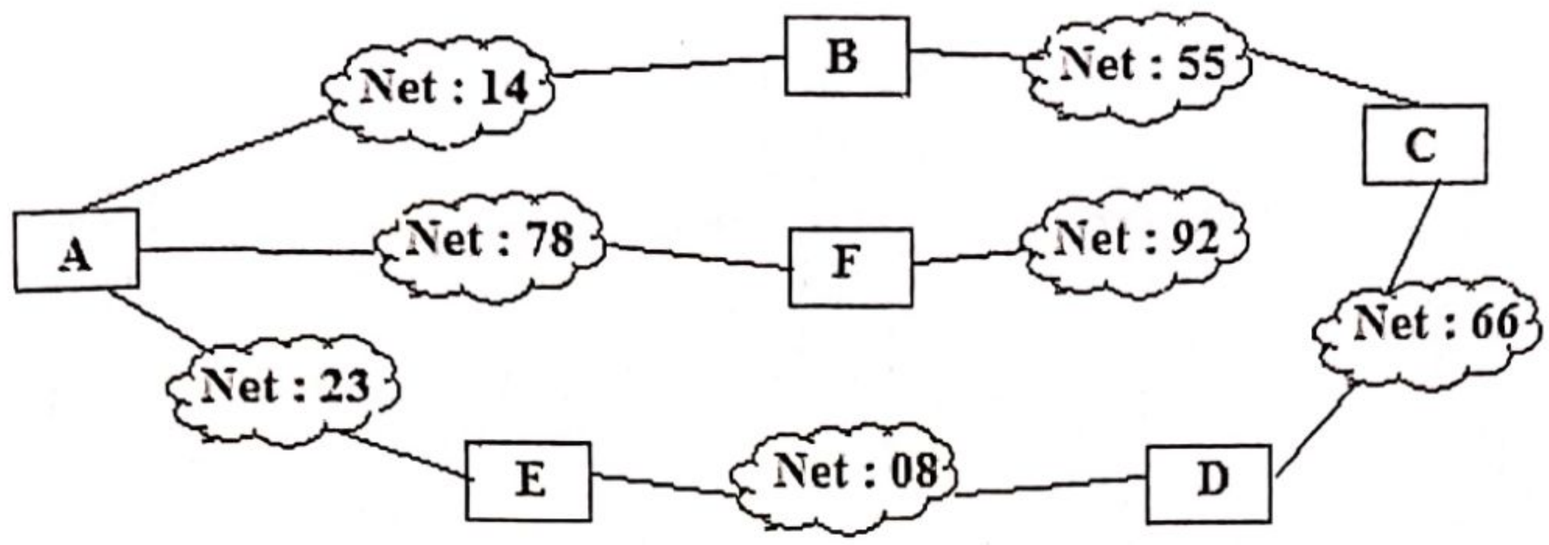


Fig: Example of an internet

The figure given below shows the first step in the algorithm. The text boxes indicate the relationship of the routers in above figure to their neighbors. Each router sends information about the internetwork only to its immediate neighbors. How, then do nonneighboring routers learn about each other and share knowledge?

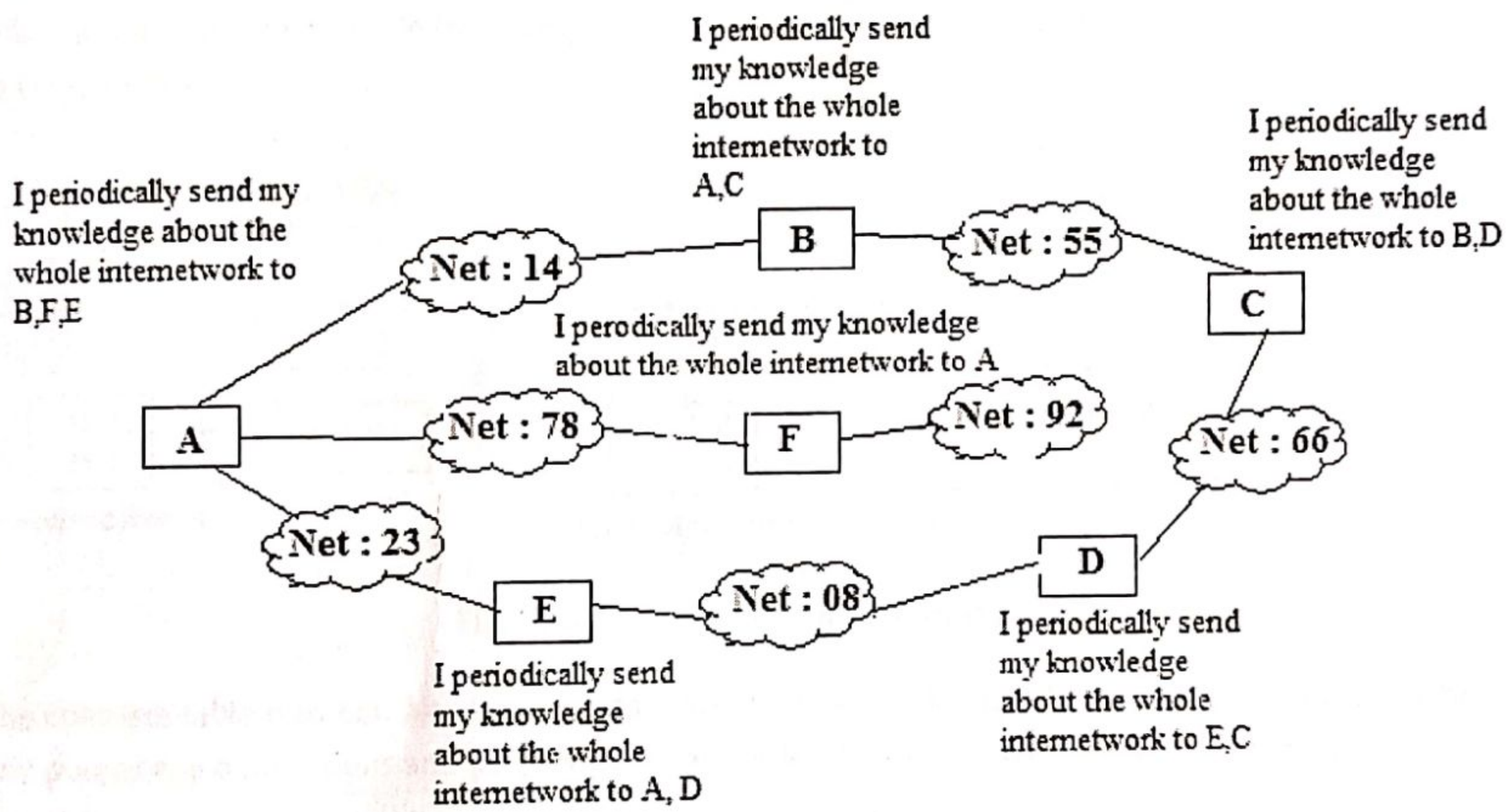


Fig: The concept of distance vector routing

A router sends its knowledge to its neighbors. The neighbors add this knowledge to their own knowledge and send the whole table to their own neighbors. Every router knows about every other router in the internetwork. Because a router is a station on each of those LANs, it also knows the ID of each station.

Network ID	Cost	Next Hop
.....	.....	.....
.....	.....	.....

Fig: Distance Vector routing table.

Scanned with OKEN Scanner

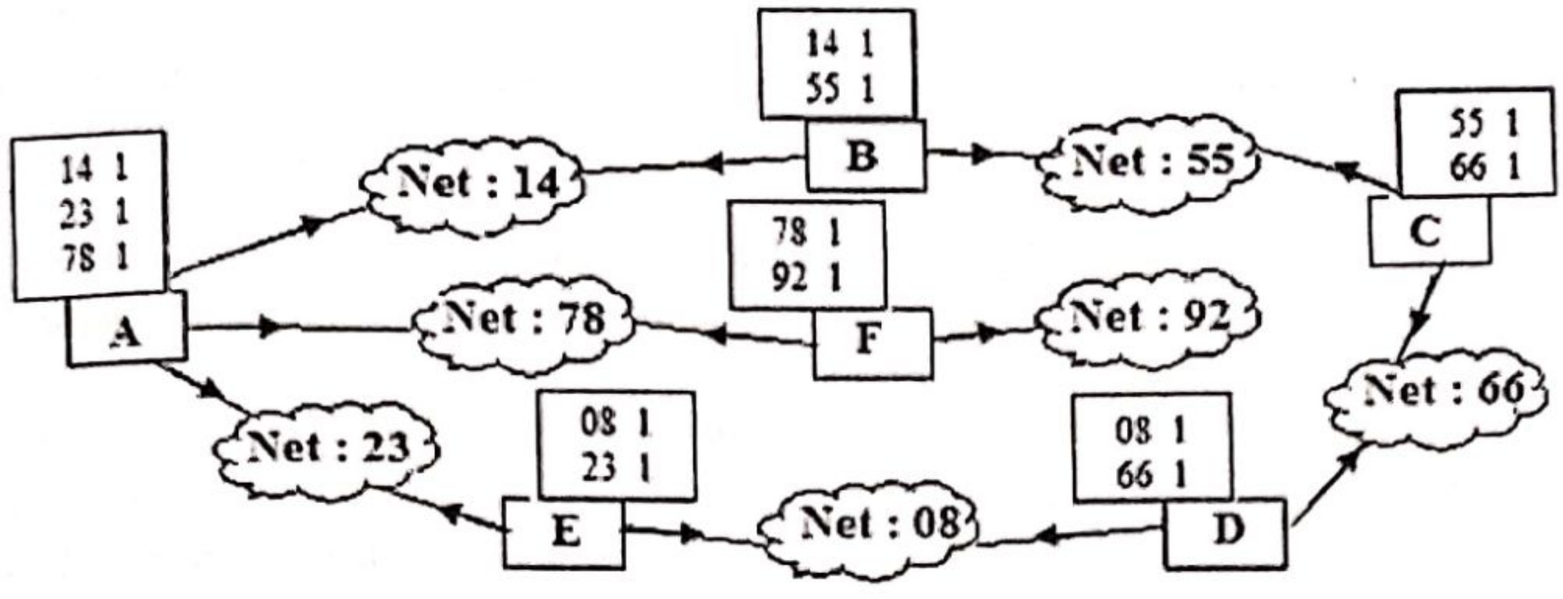


Fig: Routing Table distribution in distance vector routing

When A receives a routing table from B, it uses the information to update its own table. It says to itself: I know that B is my neighbor, so my packets can reach B in one hop. So if I add one hop to all of the costs shown in B's table, the sum will be my cost for reaching those networks. Therefore, A adjusts the information shown in B's table by adding one to each listed cost. It then combines this table with its own to create a new.

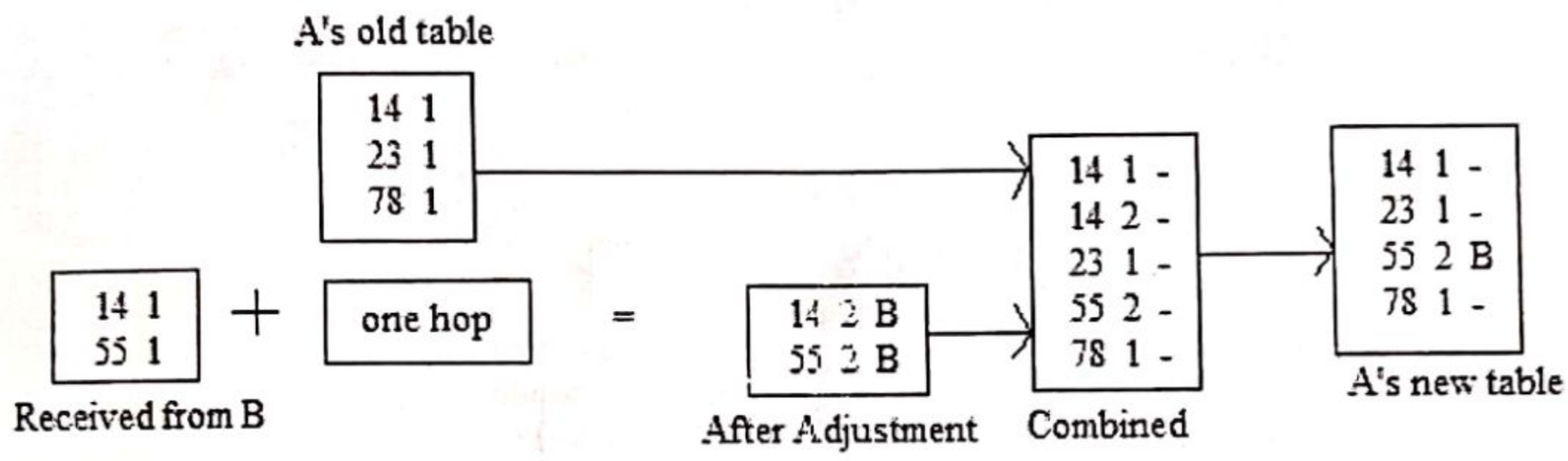


Fig: Updating routing table for router A

The combine table may contain duplicate data for some network destinations. Router A therefore finds and purges any duplications and keeps whichever version shows the lowest cost. This process continues for all routers.

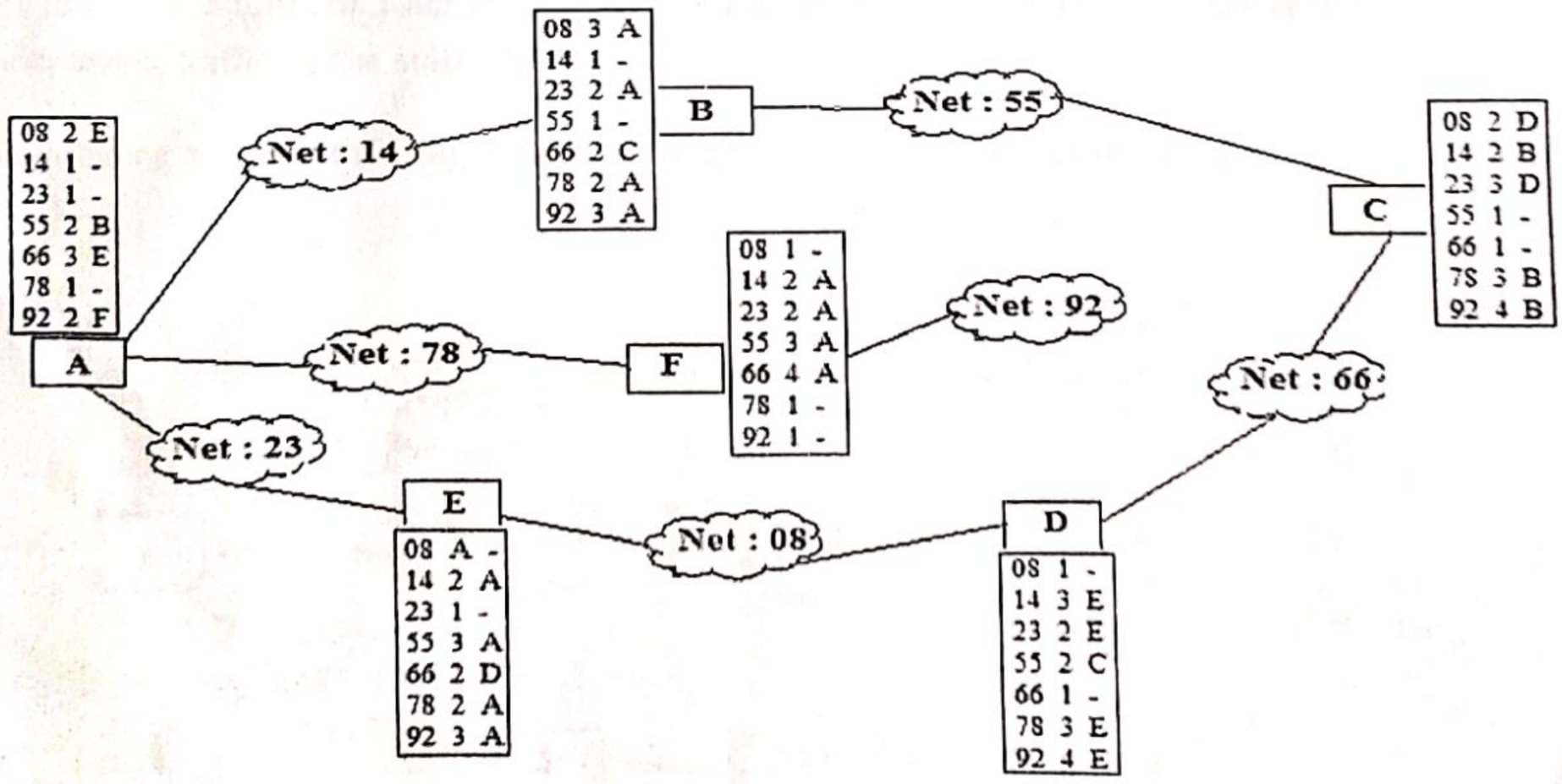


Fig: Final routing table

Scanned with OKEN Scanner

Link State Routing

In this each router shares its knowledge of its neighborhood with every other router in the internetwork. The following are true of link state routing:

- **Knowledge about the neighborhood:** Instead of sending its entire routing table, a router sends information about its neighborhood only.
- **To all routers:** Each router sends this information to every other router on the internetwork, not just to its neighbors. It does so by a process called flooding. Flooding means that a router sends its information to all of its neighbors.
- **Information sharing when there is a change:** each router sends out information about the neighbors when there is a change.

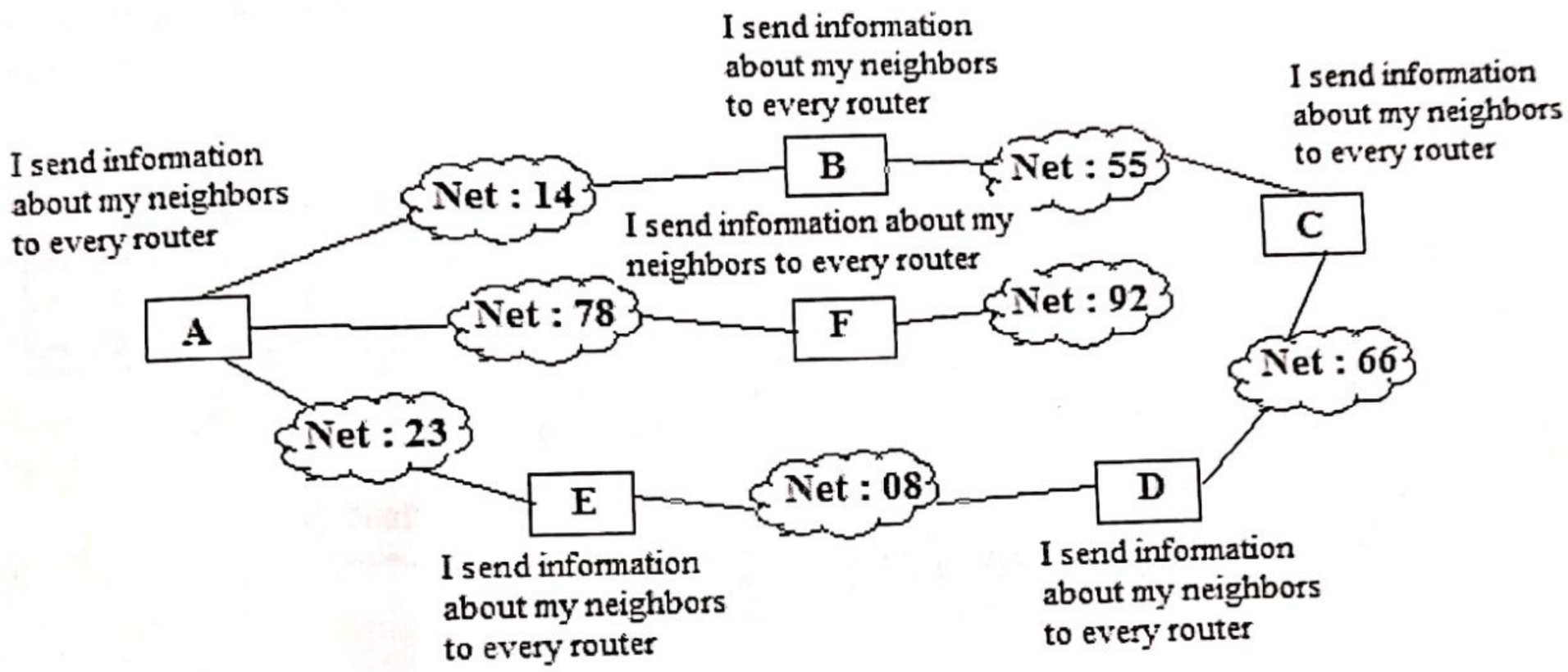
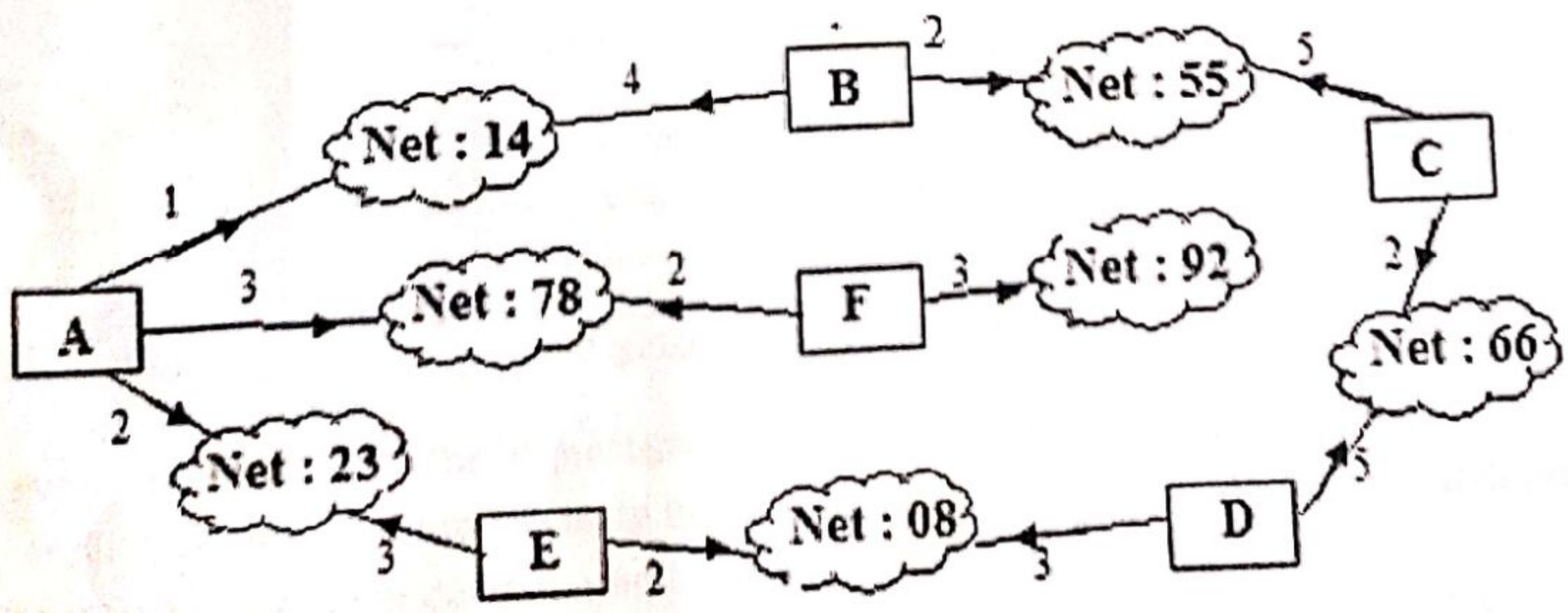


Fig: concept of link state routing

The first step in link state routing is information sharing. Each router sends its knowledge about its neighborhood to every other router in the internetwork.

Both distance vector and link state routing are lowest-cost algorithm. In distance vector routing, cost refers to hop count. In link state routing, cost is a weighted value based on a variety of factors such as security levels, traffic, or the state of the link.

In determining a route, the cost of a hop is applied to each packet as it leaves a router and enters a network.



Scanned with OKEN Scanner

Fig: Cost in Link state routing

When router floods the network with information about its neighborhood. It is said to be advertising. The basis of this advertising is a short packet called a link state packet (LSP).

Advertiser (ID)	Network(destination ID)	Cost	Neighbor (ID)
.....	.....	.....	.....
.....	.....	.....	.....

Fig: Link state packet

A router gets its information about its neighbor by periodically sending them a short greeting packet. If the neighbor responds to the greeting as expected, it is assumed to be alive and functioning. If it does not, a change is assumed to have occurred and the sending router then alerts the rest of the network in its next LSP.

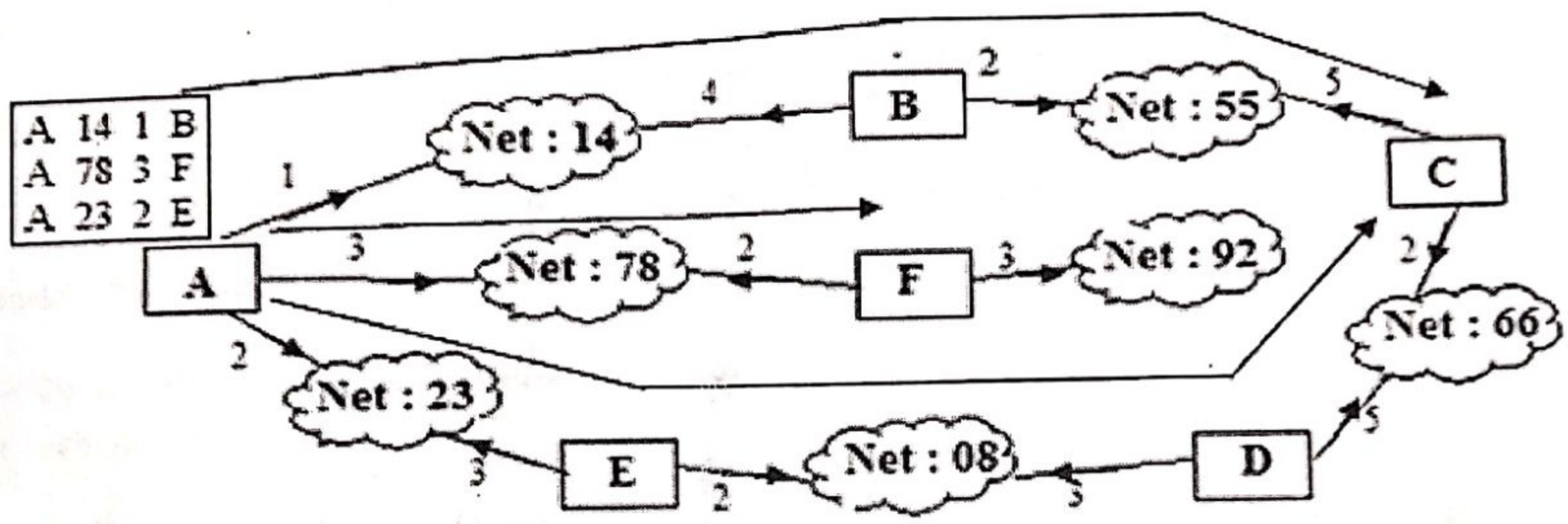


Fig: Flooding of A's LSP

Every router receives every LSP and puts the information into link state database.

Advertiser	Network	Cost	Neighbor
A	14	1	B
A	78	3	F
A	23	2	E
B	14	4	A
B	55	2	C
C	55	5	B
C	66	2	D
D	66	5	C
D	08	3	E
E	23	3	A
E	08	2	D
F	78	2	A
F	92	3	-

Fig: Link state database

Because every router receive the same LSPs, every router builds the same database. It stores this database on its disk and uses it to calculate its routing table. If a router is added to or deleted from the system, the whole database must be shared for fast updating.

Scanned with OKEN Scanner

Dijkstra Algorithm

This algorithm calculates the shortest path between two points on a network using a graph made up of nodes and arc. Nodes are of two types: networks and routers. Arcs are the connection between a router and a network. Cost is applied only to the arc from router to network. The cost of the arc from network to router is always zero.

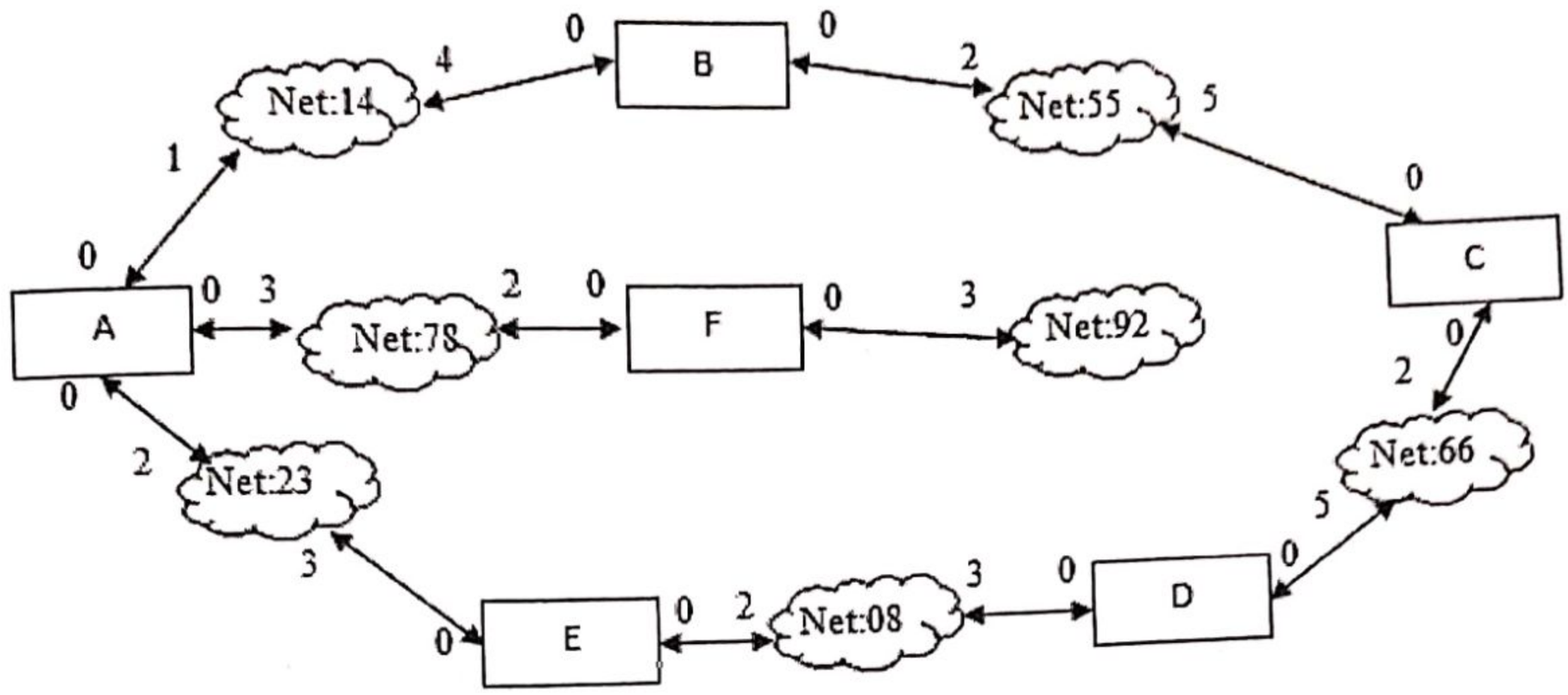
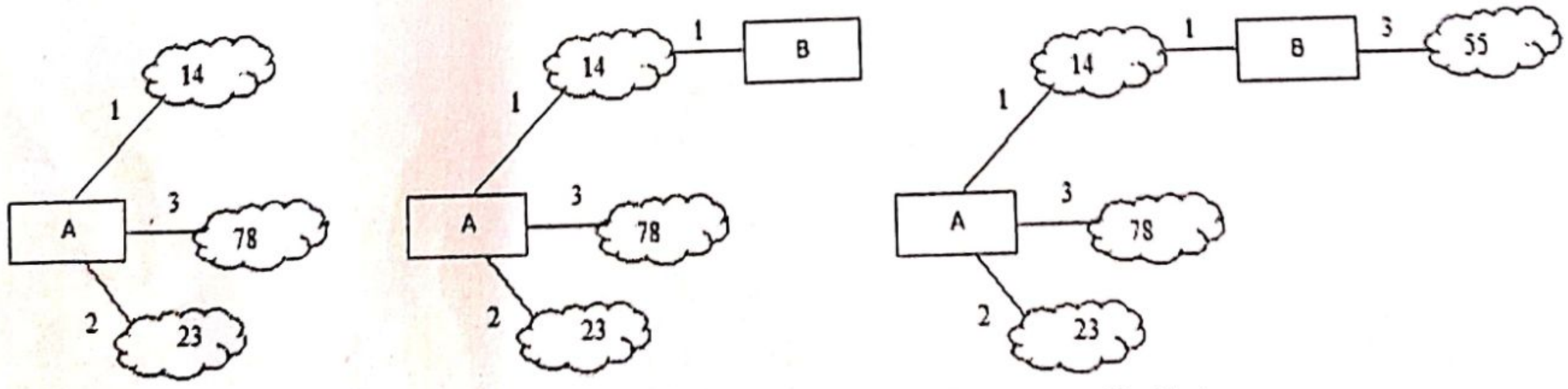


Fig: Costs in the Dijkstra algorithm

Shortest Path Tree

The Dijkstra algorithm follows four steps to discover what is called the shortest path tree (routing table) for each router.

- The algorithm begins to build the tree by identifying its root. The root of each router's tree is the router itself. The algorithm then attaches all nodes that can be reached from that root.
- The algorithm compares the tree's temporary arcs and identifies the arc with the lowest cumulative cost. This arc and the node to which it connects are now a permanent part of the shortest path three.
- The algorithm examines the database and identifies every node that can be reached from its chosen node. These node and their arcs are added temporarily to the tree.
- The last two steps are repeated until every node in the network has become a permanent part of the tree. The only permanent arcs are those that represent the shortest route to every node.

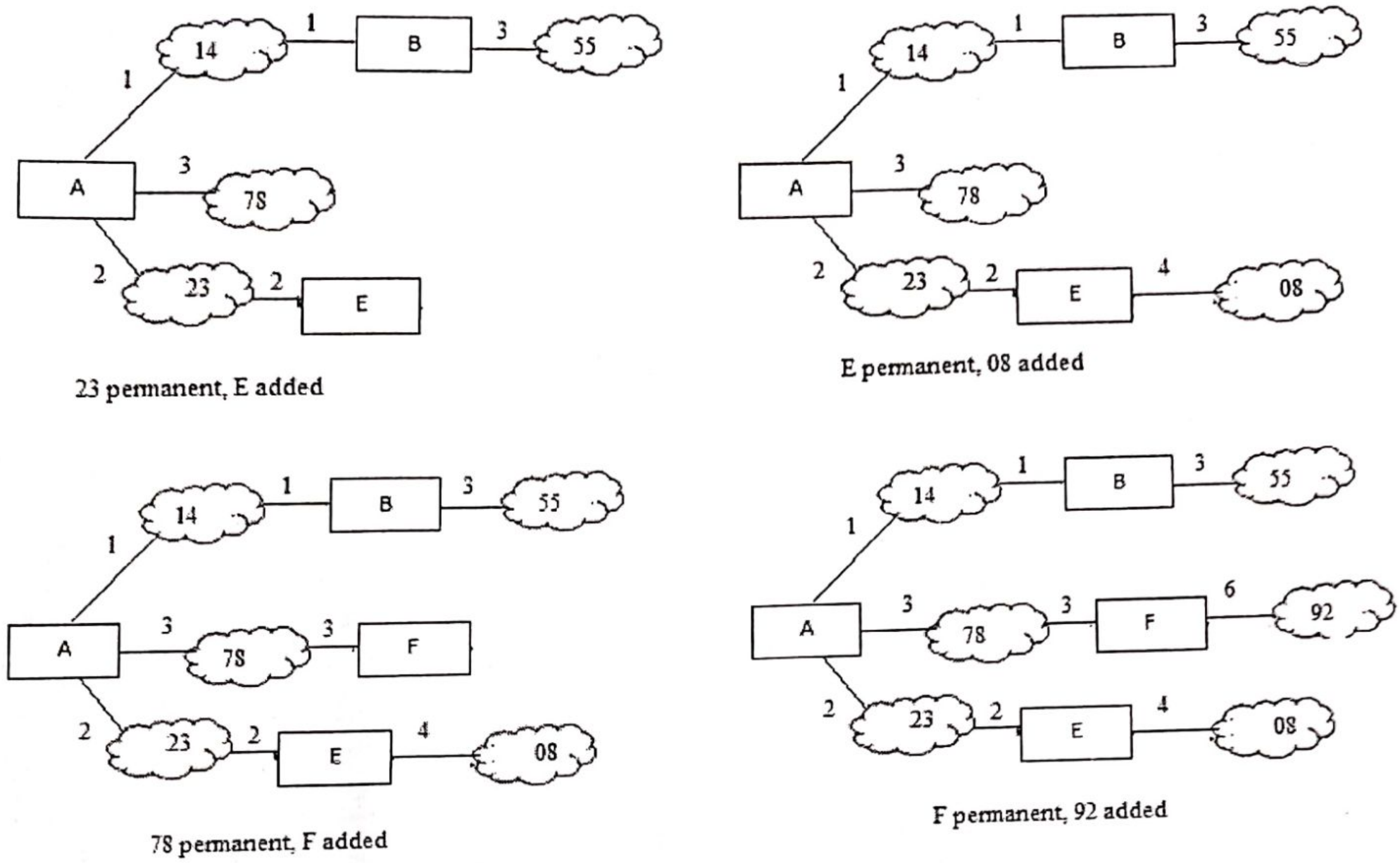


Root is A, networks 14,78,23

14 permanent , B added

B permanent, 55 added

Scanned with OKEN Scanner



23 permanent, E added

E permanent, 08 added

78 permanent, F added

F permanent, 92 added

Fig: Shows the completion of the shortest path tree for router A

Each router now uses the shortest path tree to construct its routing table.

Net	Cost	Next router
08	4	E
14	1	
23	2	
55	3	B
66	5	B
78	3	
92	6	F

Fig: Link State routing table for router A

Scanned with OKEN Scanner

Lalit (1)

Internetworking devices or Network connecting device: Areas follows.

1. Repeater
2. HUB
3. Bridges
4. Switches
5. Routers
6. Gateways

UNIT- III

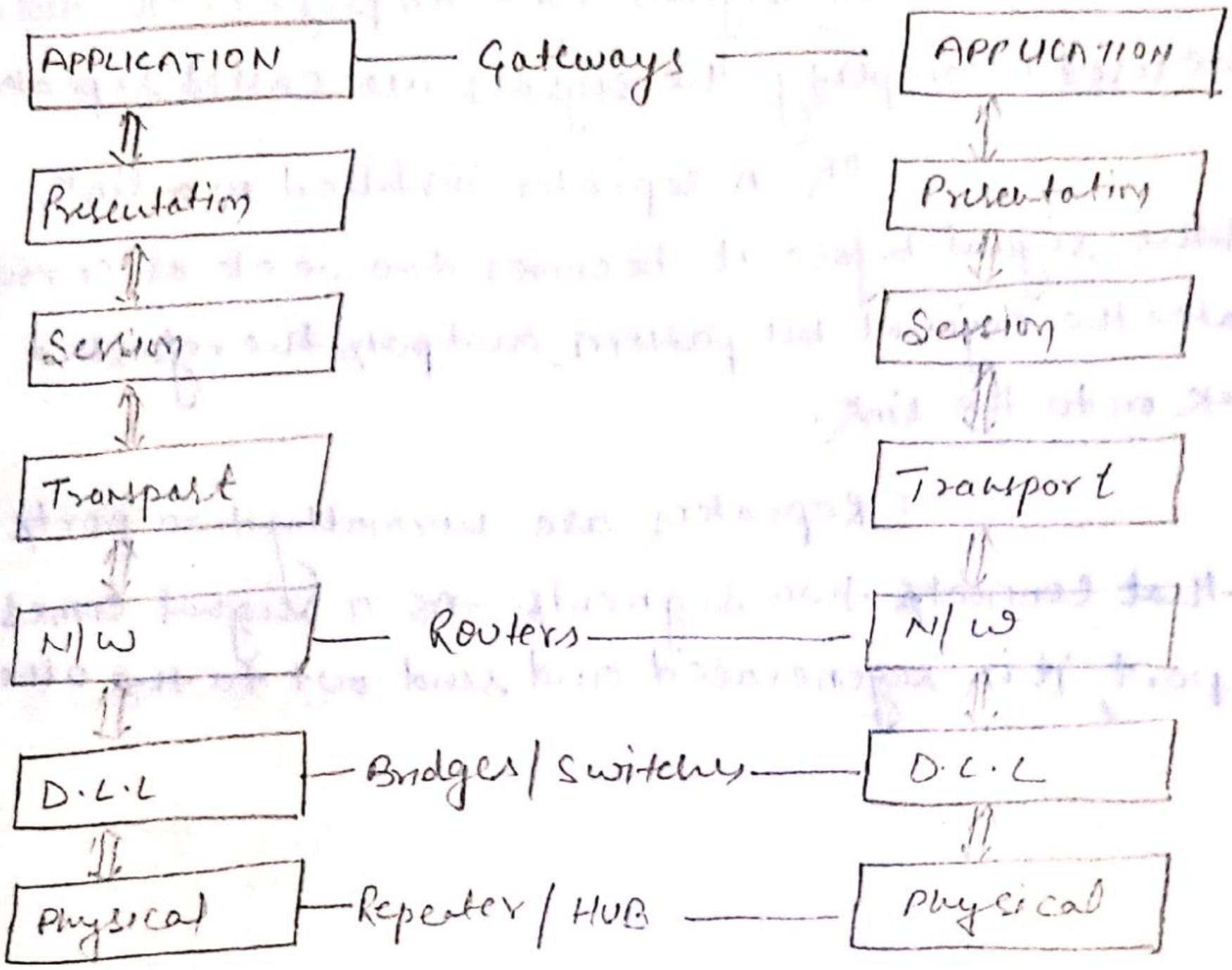


fig: Internetworking devices

NOTE: When two or more seprate networks are connected for exchanging data or resources they become an internetwork.

Routers and gateways are used for internetworking.

Repeaters and Bridges are used for Networking. Some of the connecting devices are as follows

① Repeaters:

Repeaters are used within network to extend the length of communication.

Data process through transmission media in the form of waves or signals. The transmission media weaken signals that move through it. The weaking of signal is called attenuation. If the data is to be transmitted beyond the maximum length of a communication media signals have amplified. The devices that are used to amplify the signals are called repeaters.

(OR, A repeater installed on a link receives the signal before it becomes too weak or corrupted, regenerates the original bit pattern, and puts the refreshed copy back on to the link.)

= Repeaters are normally two ports boxes that connects two segments. As a signal comes in one port, it is regenerated and send out to the other port. =

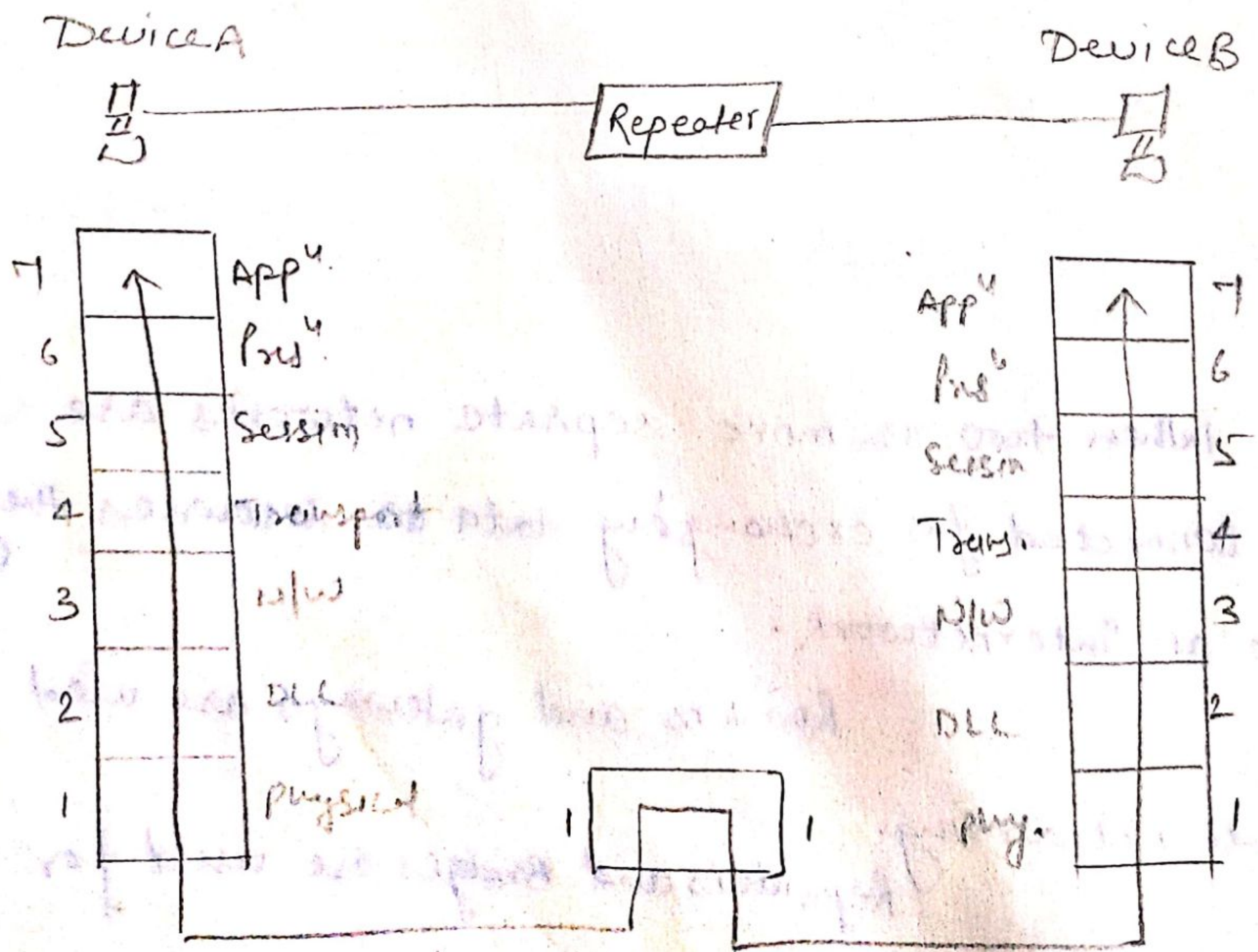


fig: A Repeater in the OSI model

Repeaters work at the Physical layer of OSI model.

Advantages:

1. Repeaters easily extend the length of N/W.
2. It can connect signals from the same network type that use different types of Cables.

Disadvantages:

1. Repeaters Can not be used to connect segments of different network types.
2. They cannot be used to segment traffic on a network to reduce congestion.

(2) HUB: Hubs are basically multiports repeaters for U.T.P. (Unshielded-twisted pair) Cables. The HUB Connects workstations and sends every transmission to all the connected workstations.

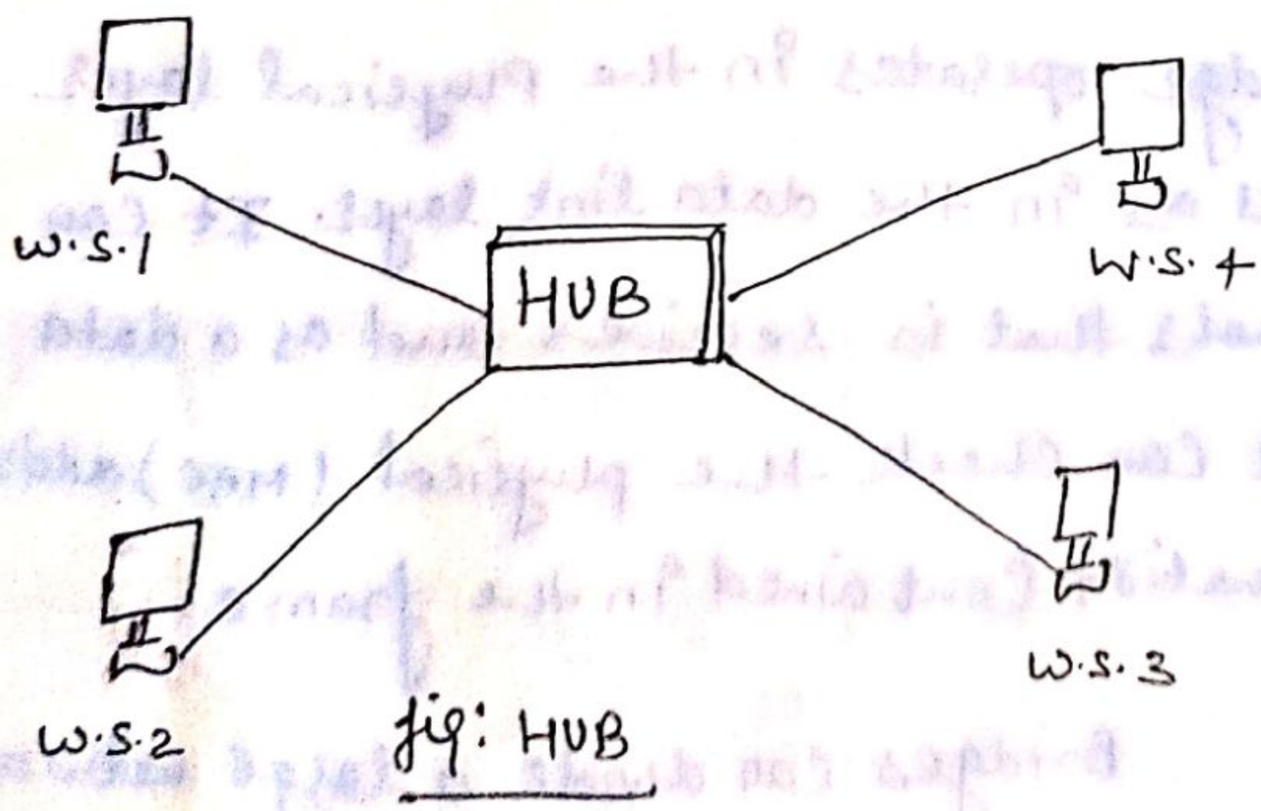


fig: HUB

There are three main types of HUB: (HUB can be divided as:)

1. Passive HUBS
2. Active HUBS
3. Intelligent HUB

1. Passive HUB: A passive hub simply combines the signals of a network segments. There is no signal processing or regeneration, with a passive HUB, each computer receive the signals sent from all the other computers connected to the HUB.

2. Active HUB: It acts as repeaters and regenerates the data signals to all ports. By using active HUBS the distance between devices can be increased.

3. Intelligent HUB: In addition to signal regeneration, intelligent HUBS perform some network management and intelligent path selection. A switching HUB chooses only the port of the device where the signal need to go, rather than sending the signals along all paths. HUBS can also be used to create multiple levels of Hierarchy.)

(3) Bridges: A Bridge operates in the physical layer as well as in the data link layer. It can regenerate the signals that is receives and as a data link layer device, it can check the physical (MAC) address of source and destination contained in the frame.

(1) = (Bridges can divide a large network into smaller segments. They can also relay frames between two originally seprate LAN's. Unlike repeaters, however bridges contain logic that allow them to keep the traffic for each segment seprate. In this way,

they filter traffic, a fact that makes them useful for controlling congestion and isolating problem links. Bridges can also provide security through this partitioning of traffic. (1)

(2) A bridge operates at the DLL, giving it access to the physical addresses of all stations connected to it. When a frame enters a bridge, the bridge not only regenerates the signal but checks the address of the destination and forwards the new copy only to the segment to which the address belongs. (2)

(3) The major difference between the bridge and repeater is that the bridge has a filtering capability. That means it can check the destination address of a frame and decide if the frame should be forwarded or dropped. (3)

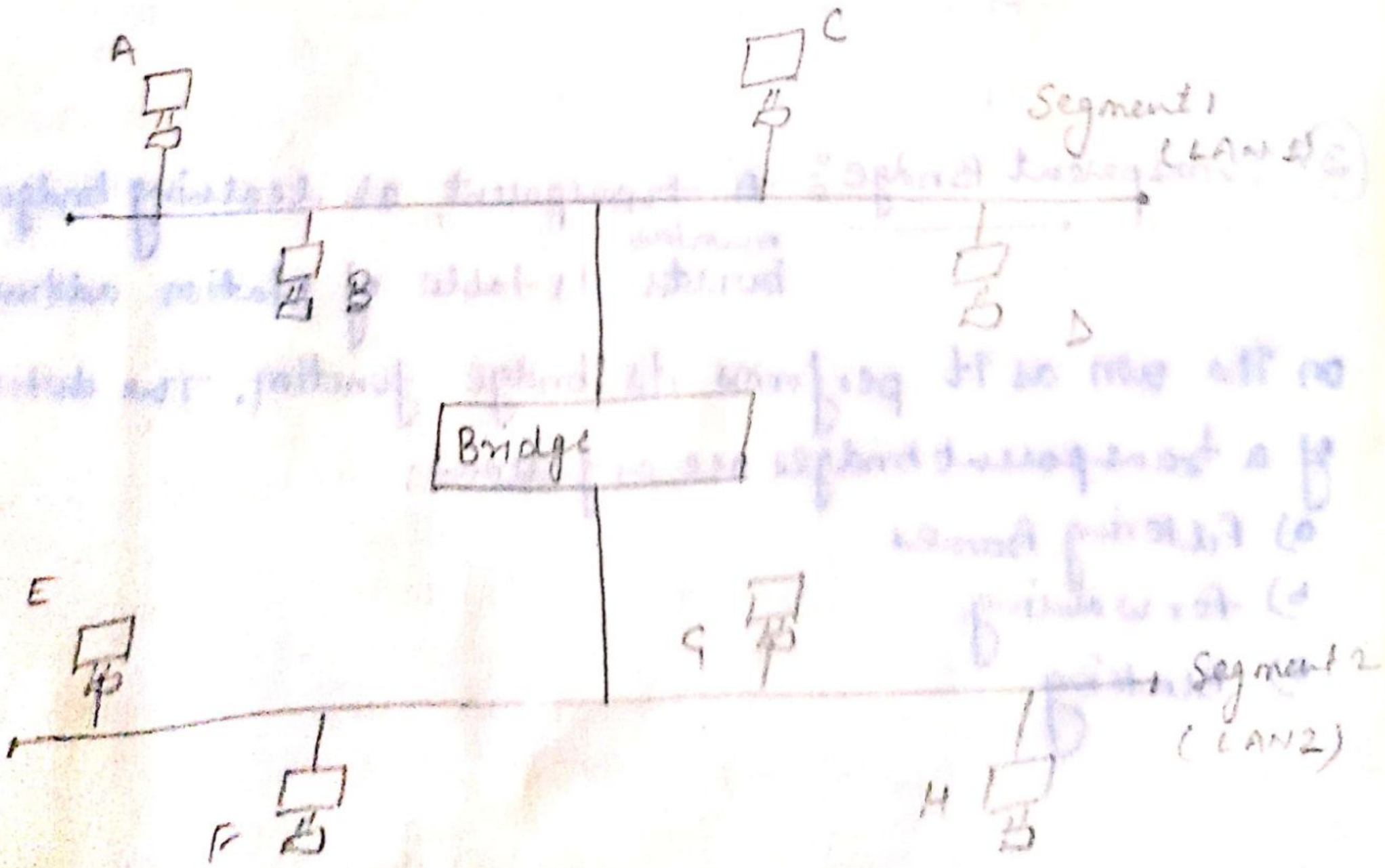


fig: A Bridge

Types of Bridges:

(1) **Simple Bridge:** Simple Bridges are the most primitive and least expensive type of bridge. A simple bridge links two segments and contains a table that lists the addresses of all the stations included in each of them.

(2) **Multiport Bridge:** A multiport bridge can be used to connect more than two LANS. ~~AND each one holding~~ In this figure, the bridge has contain three tables, each one holding the physical addresses of stations reachable through the corresponding port.

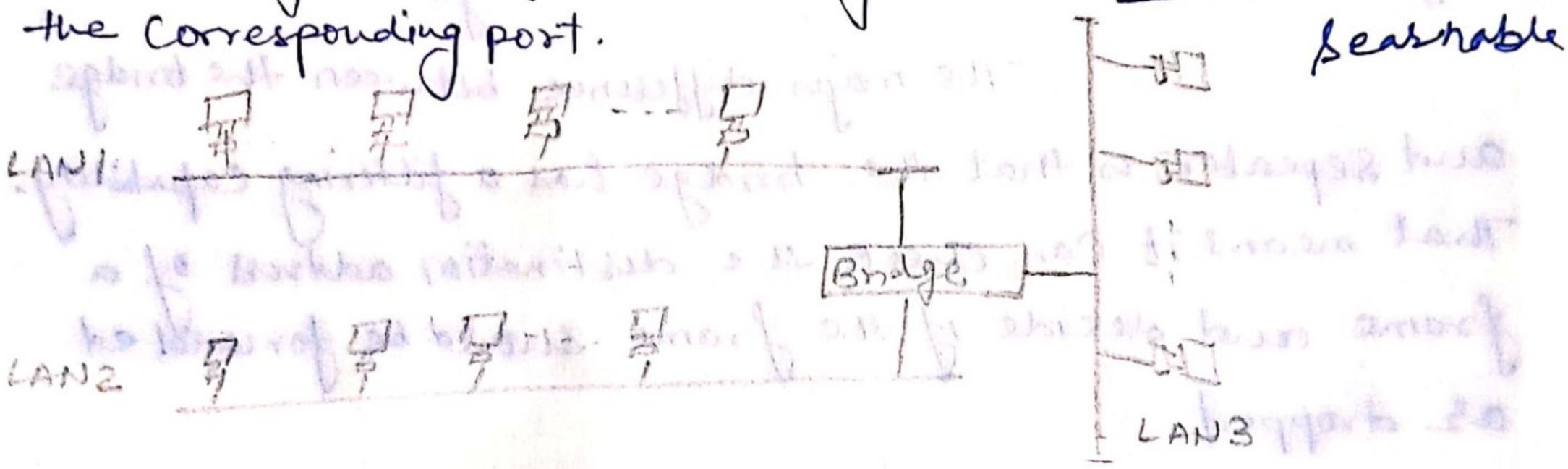


fig. Multiport Bridge

(3) **Transparent Bridge:** A transparent, or learning bridge maintains its table of station addresses on its own as it performs its bridge function. The duties of a transparent bridges are as follows:

a) Filtering frames
b) forwarding
c) Blocking

(4.) **Switches**: "One way of relieving network congestion is to use a switch, either in place of a HUB or Bridge. It is a point to point device and it operates at DLL.

Switches allows each work station to transmit information over the network independent of the other work stations. These transmissions b/w computers may be simultaneous. As opposed to HUBS, switches are more like the modern telephone system where several private conversations take place at one time."

Some switches can operate at different speeds, allowing the connection of cables using different bandwidths (10 mbps and 100 mbps).

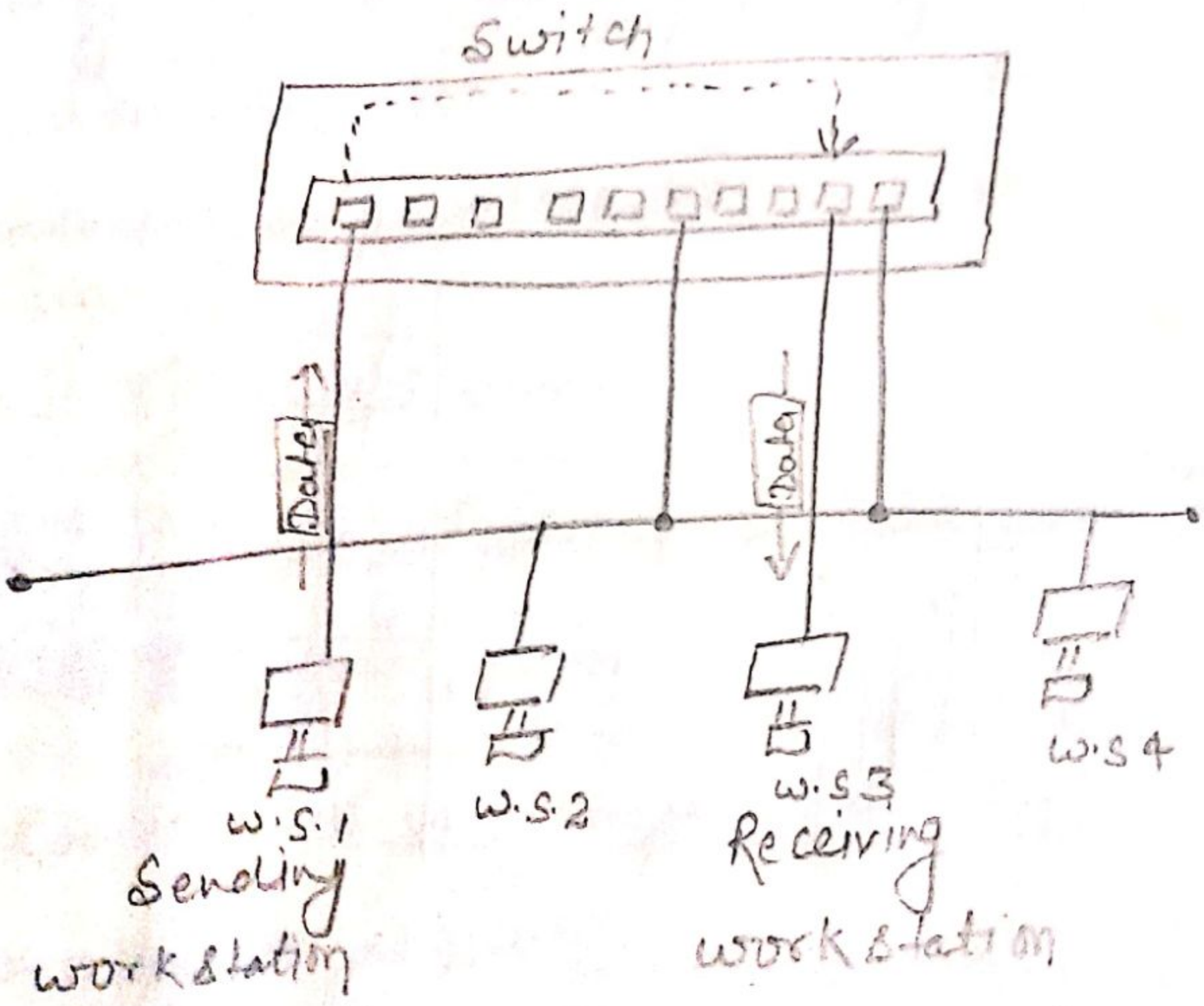


fig: Switches direct infor^n. to specific workstations

(5) **Routers**:- "Routers are devices which connect two or more networks that use similar protocal. A router consists of Hardware and software. Hardware can be a computer is specific device. and software consists of special management programs that control flow of data between networks.

A router receives packets and select the optimum path to forward the packet across the network. Router build a table of all the device addresses (routing table) across the networks. using this table, the router forwards a transmission from the sending station to the receiving station across the best path.

Routers operates at a n/w layer of the O.S.I model.

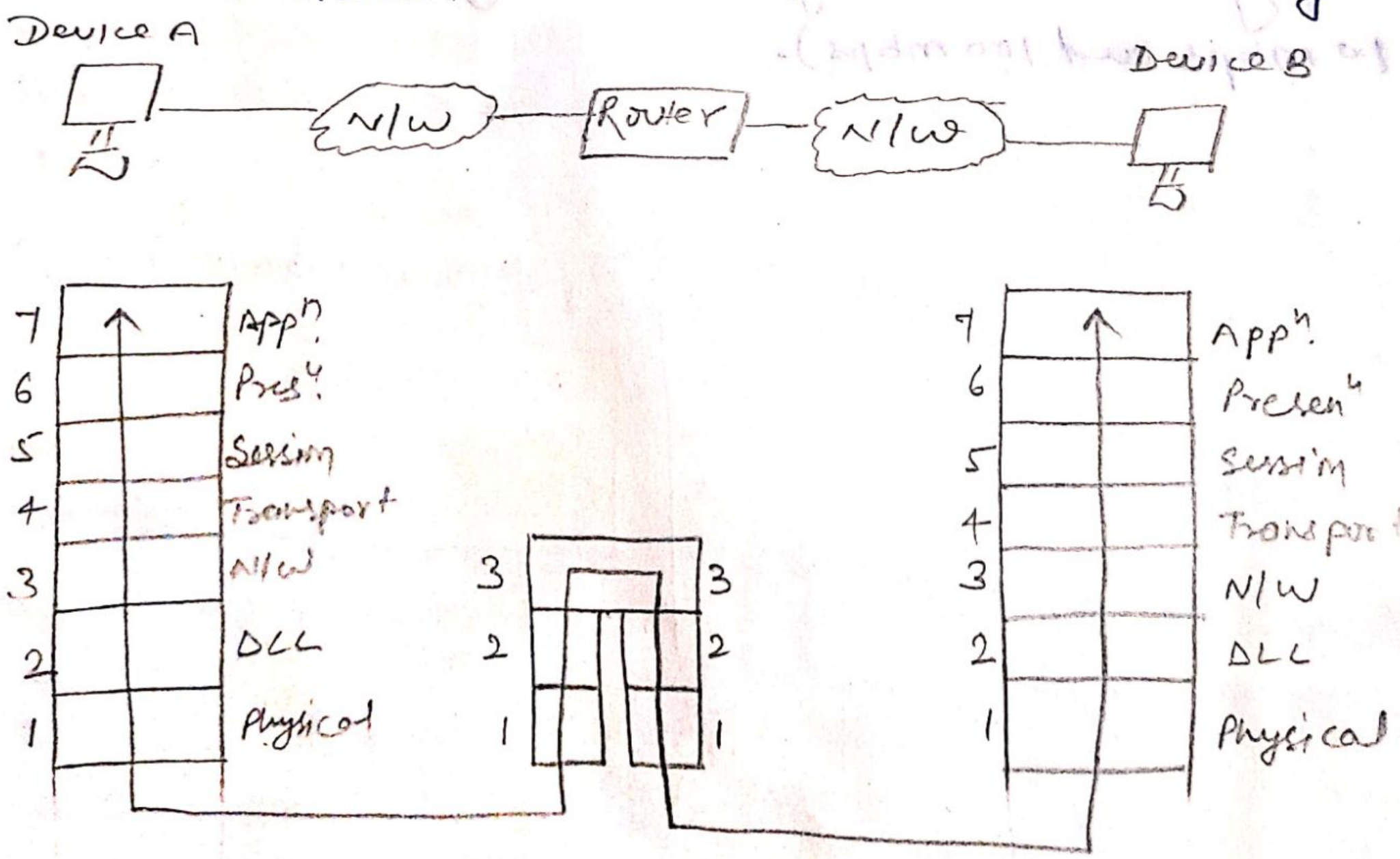


fig: A router in the OSI model

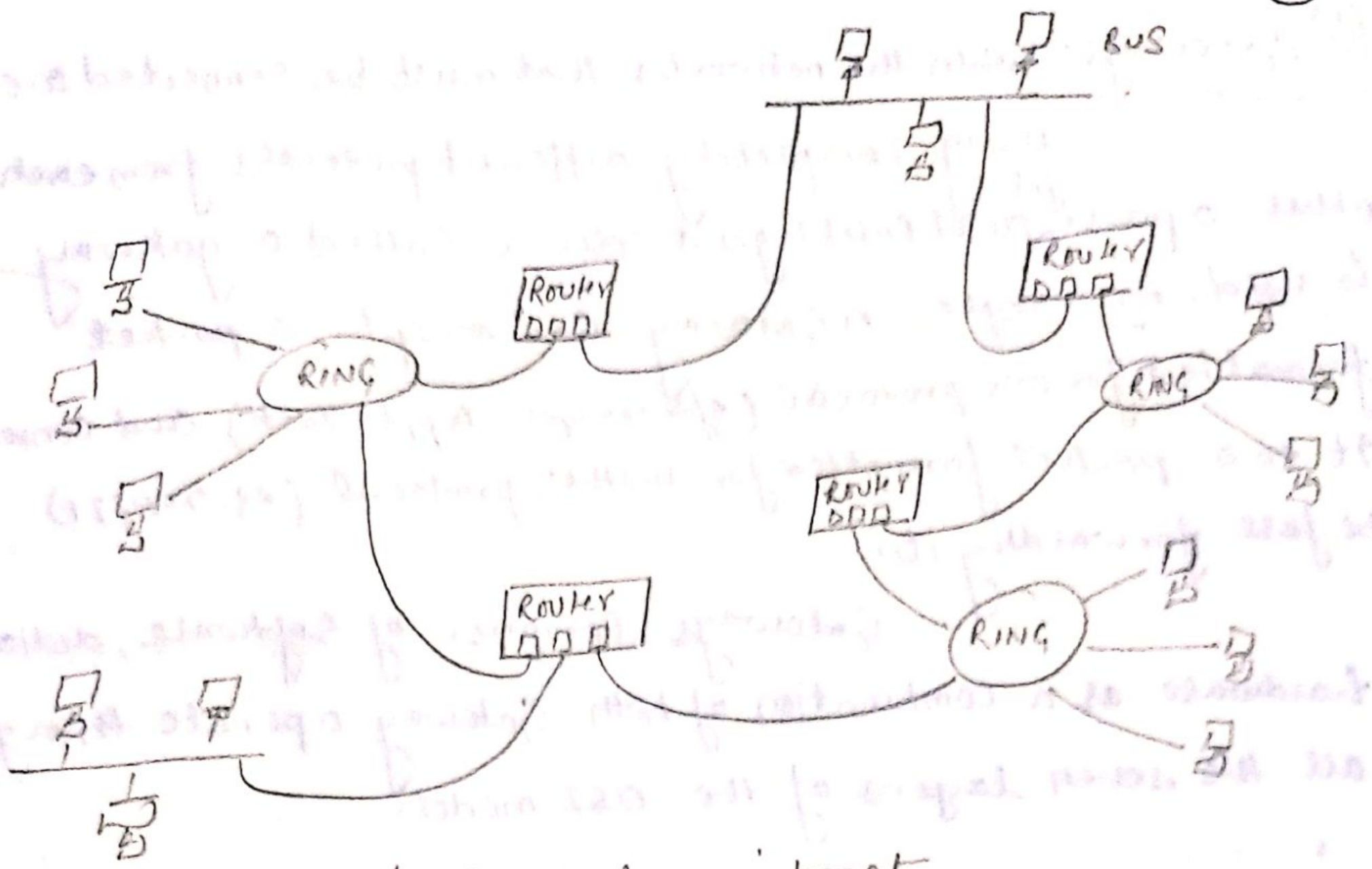


fig Routers in an internet

Advantages of Router:

1) They use high level of intelligence to rout data.
2) Routers can also act as a bridge to handle non rout able protocals) such as NetBEUI (N/W Bios extended user Interface).

Disadvantages of Router:

1) High level of intelligence take more processing time which can effect performance.
2) Routers are very complicated which installation and maintenance difficult.

Scanned with OKEN Scanner

(6) Gateways: When the networks that must be connected are using completely different protocols from each other, a powerful and intelligent device called a gateway is used. For example, A Gateway can accept a packet formatted for one protocol (e.g. for example AppleTalk) and convert it to a packet formatted for another protocol (e.g. TCP/IP) before forwarding it.

Gateways comprise of software, dedicated hardware or a combination of both. Gateway operate through all the seven layers of the OSI model.

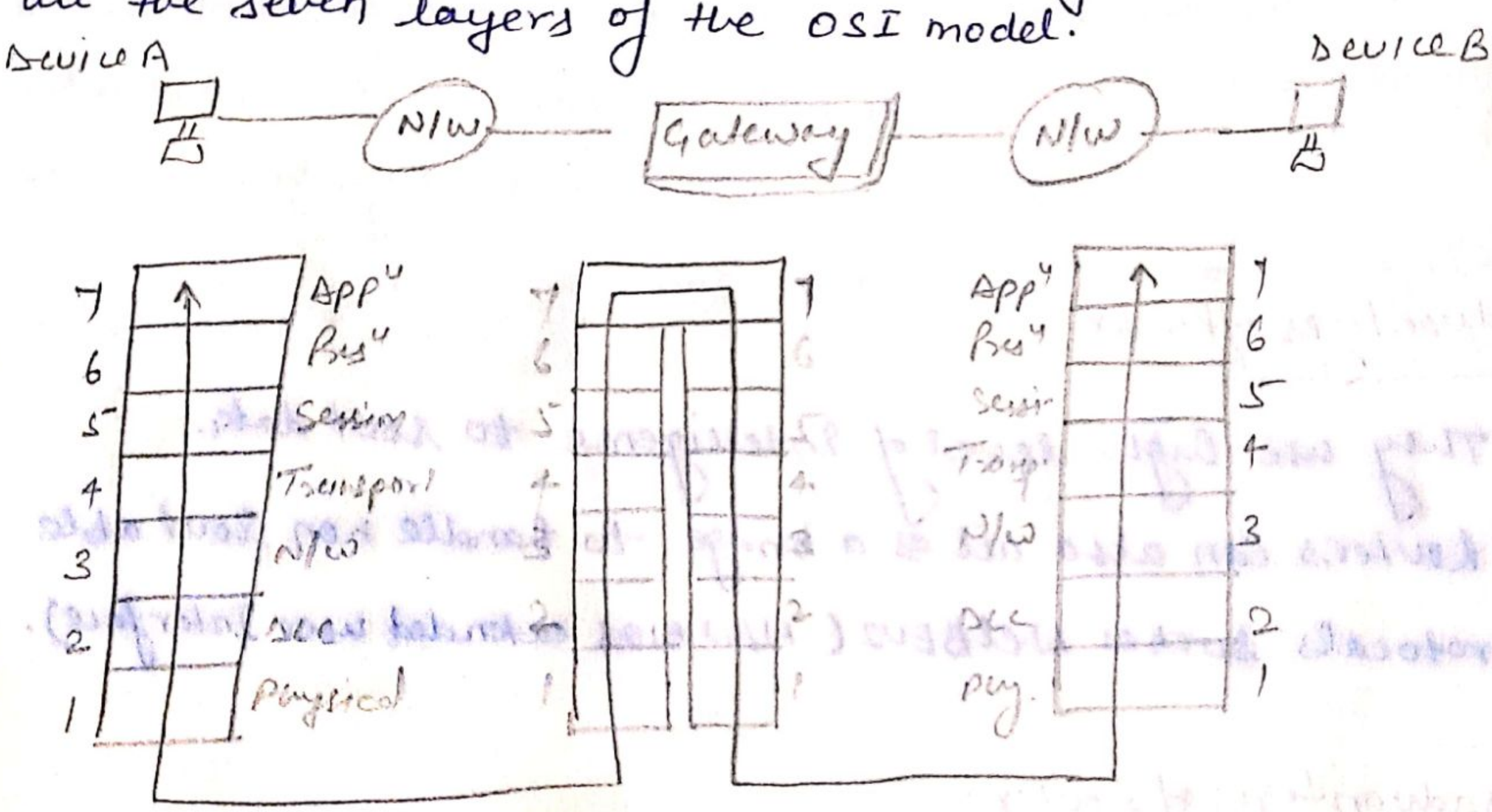


fig: A Gateway in the OSI model.

Gateways can connect systems with different com^n protocols & Architecture. for exa

* A Gateway connecting an SNA (System N/W Architecture) n/w (IBM) to a Netware network (Novell).

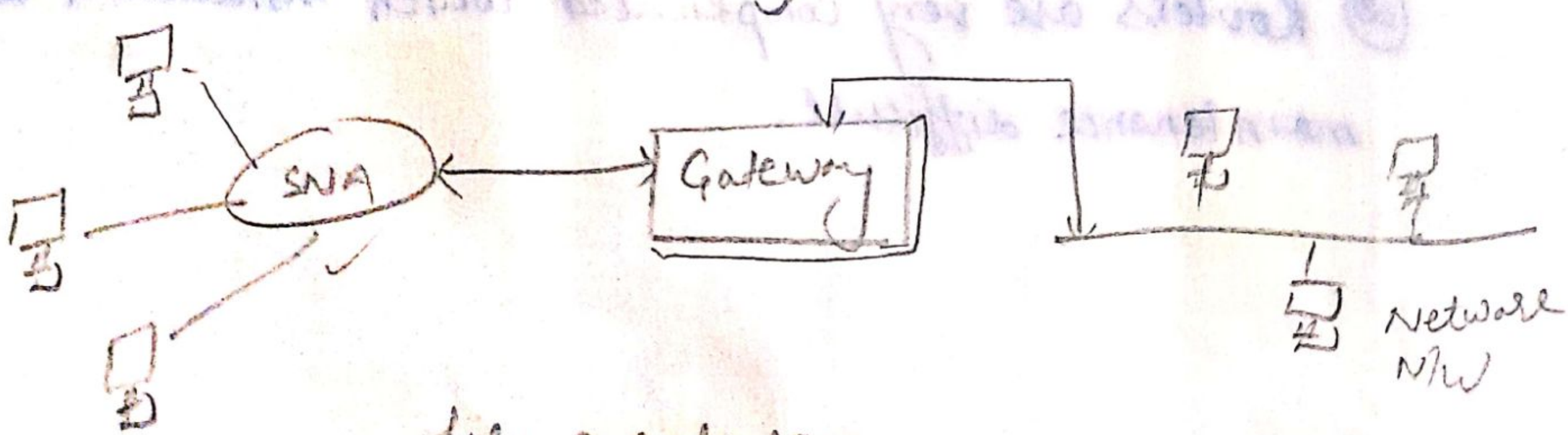


fig: A Gateway

Congestion:- An important issue in a packet-switched network is congestion. Congestion in a network may occur if the load on the network (the number of packets sent to the network) is greater than the capacity of the network (the number of packets a network can handle). Congestion control refers to the mechanism and techniques to control the congestion and keep the load below the capacity.)

Congestion in a Network or Internetwork occurs because routers and switches have queue-buffers that hold the packets before and after processing. When a packet arrives at the incoming interface, it undergoes three steps before departing.

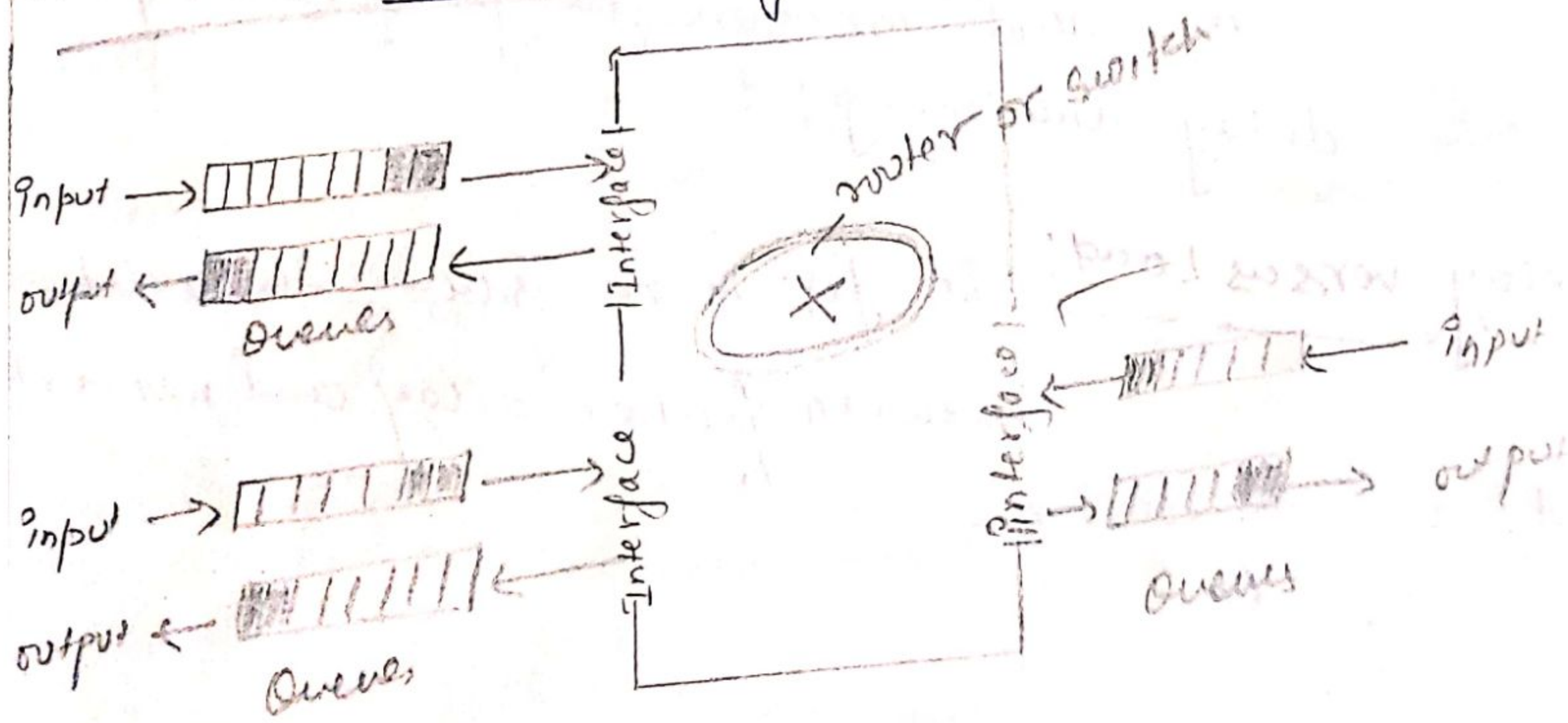


fig Incoming Packet

Step1: The packet is put at the end of the input queue while waiting to be checked.

Step2: The processing module of the router removes the packet from the input queue once it reaches the

front of the queue and uses its routing table and the destination address to find the route.

Step3: The packet is put in the appropriate output queue and wait its turn to be sent.

We need to be aware of Two issues

First, if the rate of packet arrival is higher than the packet processing rate, the input queues become longer and longer.

Second, if the packet departure rate is less than the packet processing rate, the output queue become longer and longer.

Network performance: Congestion control involves two factors that measure the performance of a Network: delay and Throughput.

(1) Delay versus Load: In fig: 4.26 show the relationship between packet delay and network Load.

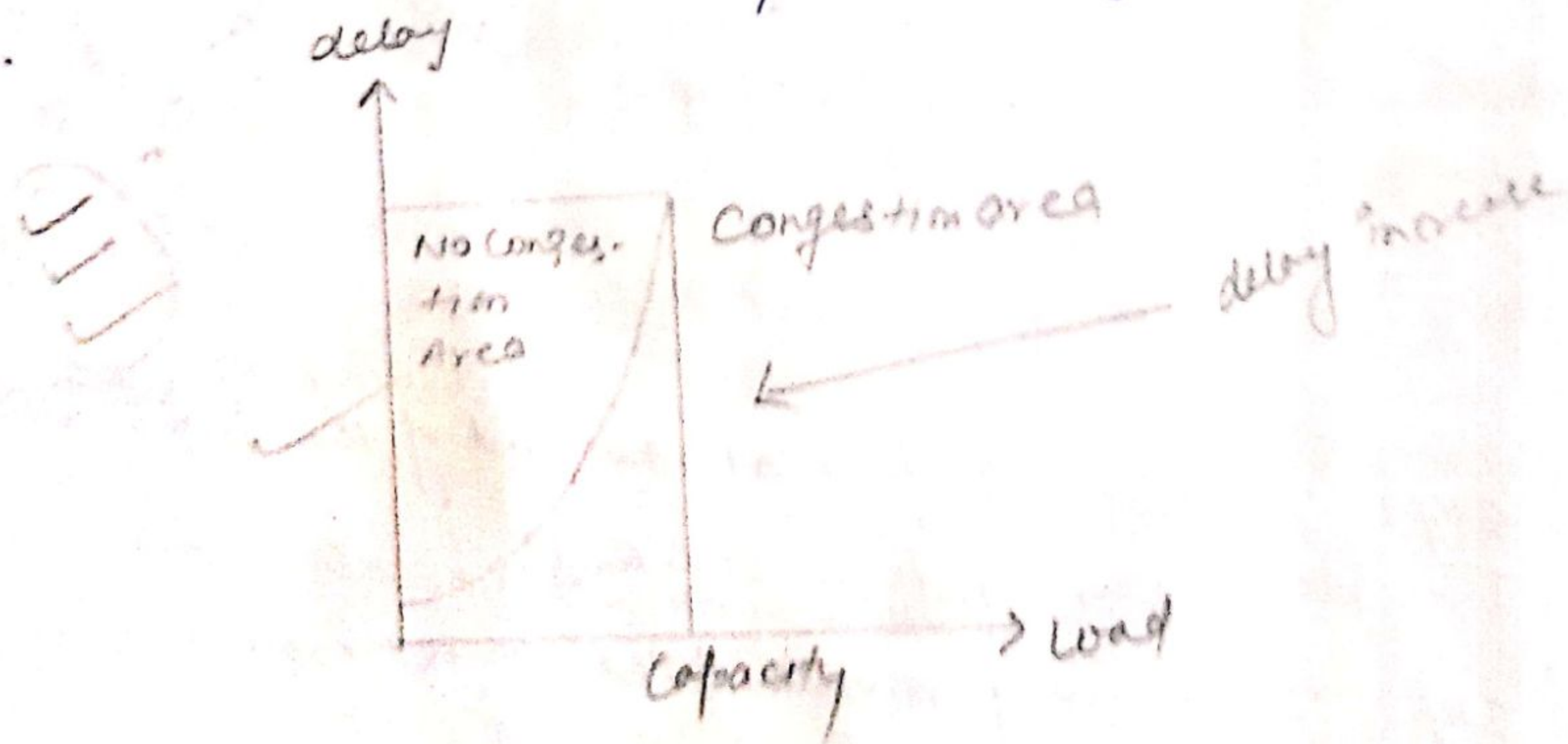


fig: Packet delay and Network Load

Note that when the load is much less than the capacity of the network, the delay is at a minimum. This minimum delay is composed of propagation delay and processing delay.

However, when the load reaches the network capacity, the delay increases sharply because we now need to add the waiting time in the queues (for all routers in the path) to the total delay. Note that the delay becomes infinite when the load is greater than the capacity. If this is not obvious, consider the size of queue when almost no packet reaches the destination, or reaches the destination with infinite delay; the queue become longer and longer. delay has a negative effect on the load and consequently the congestion. when a packet is delayed, the source, not receiving the acknowledgement, retransmits the packets, which makes the delay and the congestion, worse.

(ii) Throughput versus Load:

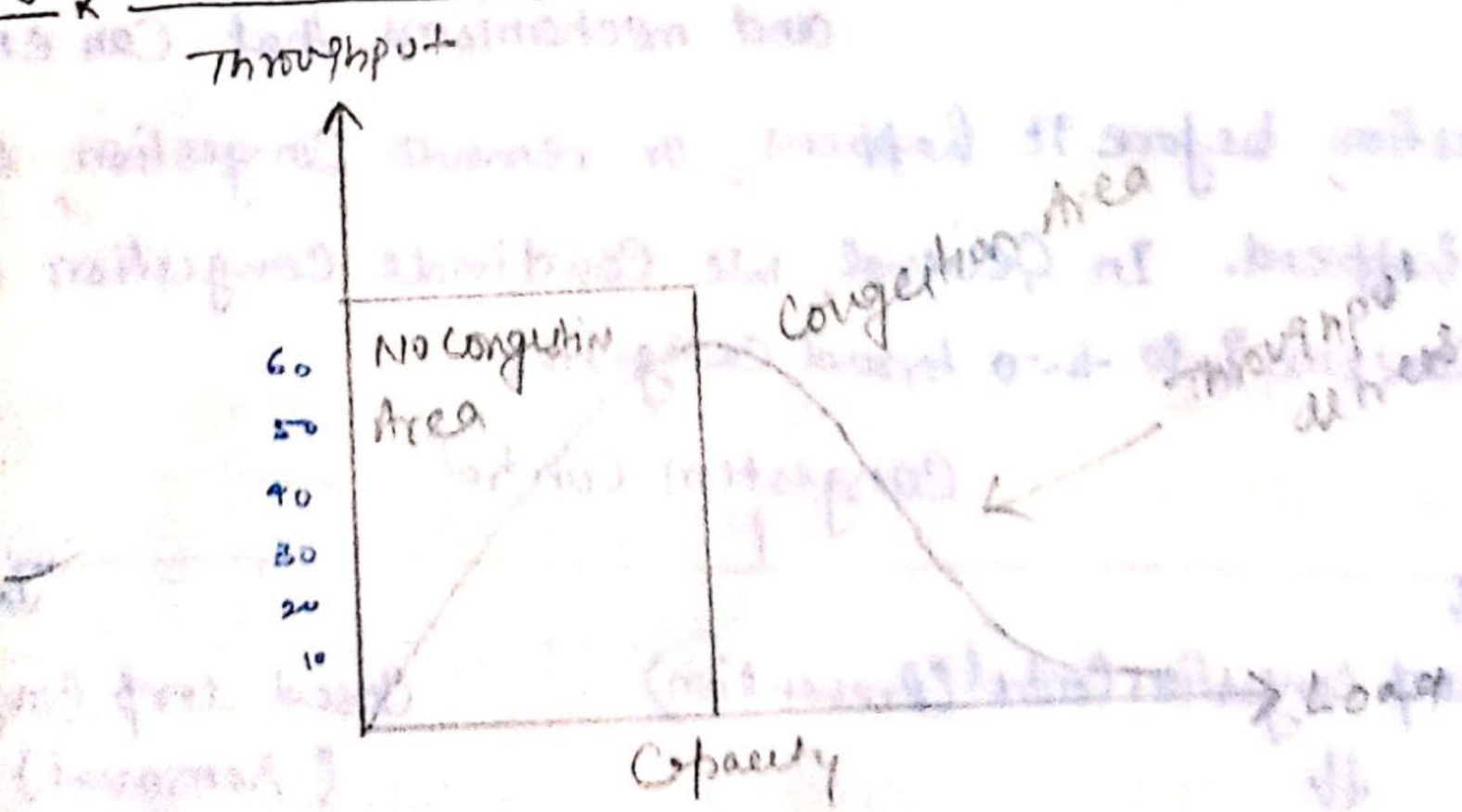


fig: Throughput versus network load

Note that when the load is below the capacity of the network, the throughput increases proportionally with the node. We expect the throughput to remain constant after the load reaches the capacity but instead the throughput declines sharply. The reason is the discarding of packets by the routers. When the load exceeds the capacity, the queue become full and the routers have to discard some packets. Discarding packets does not reduce the number of packets in the network because the sources retransmit the packets using time-out mechanisms, when the packets do not reach the destinations.

Imp

Congestion Control:

Congestion Control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happend. In General, we can divide congestion control mechanisms into two broad categories:

Congestion Control

- Open Loop Congestion Control (Prevention)
  - * Retransmission Policy
  - * Window Policy
  - * Acknowledgement Policy
  - * Discarding Policy
  - * Admission Policy
- Closed loop Congestion Control (Removal)
  - Imp * Back Pressure
  - Imp * Choke Point
  - * Implicit signaling
  - * Explicit signaling
    - Imp (i) Backward signaling
    - Imp (ii) Forward "

(1) Open-loop congestion control: In open loop congestion control, policies are applied to prevent congestion before it happens. In these mechanism, congestion control is handled by either the source or the destination. A list of policies that can prevent congestion are as explain follows:

(a) Retransmission Policy: A good retransmission policy can prevent congestion. The retransmission policy and the retransmission timers must be designed to optimize efficiency and at the same same time prevent congestion.

(b) Window policy: The type of window at the sender may also affect congestion. The selective (Repeat) Repeat window is better than the GO BACK N window for congestion control.

(c) Acknowledgement Policy: The acknowledgement policy imposed by the receiver may also affect congestion. If the receiver does not acknowledge every packet it receives, it may slow down the sender and help prevent congestion.

(D) Discarding policy: A good discarding policy by the routers may prevent congestion and at the same time may not harm the integrity of the transmission.

Scanned with OKEN Scanner

(e) Admission Policy: An admission policy, which is a quality of service mechanism, can also prevent congestion in virtual circuit network. Switches in a flow first check the resource requirement of a flow before admitting it to the network.

(2.) Closed loop congestion control: Closed loop congestion control mechanisms try to alleviate (to relieve, to comfort) / Remove congestion after it happens. Several mechanisms have been used by different protocols. Some of them are as follows:

(a) Back Presure: When a router is congested, it can inform the previous upstream router to reduce the rate of outgoing packets. The action can be recursive all the way to the router before the source. This mechanism is called Back Presure.

(b) Choke Point: A choke point is a packet send by a router to the source to inform it of congestion. This type of control is similar to ICMP's source quench packet.

(internet control message protocol)

silence

(c) Implicit signaling: The source can detect an implicit signal concerning congestion and slow down its sending rate.

For example: The more delay in receiving an acknowledgement can be a signal that the network is congested.

(d) Explicit signaling: The routers that experience congestion can send an explicit signal, the setting of a bit in a packet, for example, to inform the sender or the receiver of congestion. Explicit signaling can occur in either the forward or the backward direction.

(i) Backword signaling: The bit can be set in a packet moving in the direction opposite to the congestion. This bit can warn the source that there is congestion and that it needs to slow down to avoid the discarding of packets.

(ii) Forward signaling: The bit can be set in a packet moving in the direction of the congestion. This bit can warn the destination that there is congestion. The receiver in this case can use policies, such as slowing down the acknowledgement, to alleviate (increase) the congestion.

Quality of service: Quality of service is an internet-working issue, it has some flow characteristics, these are as follows:

(1) Reliability
(2) delay
(3) jitter
(4) Bandwidth

(1) Reliability :- Reliability is a characteristics that a flow needs. Lack of reliability means losing a packet or acknowledgement, which entails retransmission. However the sensitivity of application programs to reliability is not the same: for example, it is more important that electronic mail, file transfer, and Internet access have reliable transmissions than telephony or audio conferencing.

(2) Delay: Source to destination delay is another flow characteristic. Again application can tolerate delay in different degrees. In this case, telephony, audio conferencing, video conferencing, and remote log-in need minimum delay, while delay in file transfer or e-mail is less important.

(3) Jitter :- Jitter is the variation in delay for packets belonging to the same flow. Real time audio and video cannot tolerate high jitter. For example, a real time video broadcast is useless if there is a 2 ms. delay for the first and second packets and a 60 ms delay for the third and forth.

On the other hand, it does not matter if packets carring information in a file

have different delays. The transport layer at the destination waits until all packets arrive before delivery to the application layer.

(4) Bandwidth: Different applications need different bandwidths. In video conferencing we need to send millions of bits per second to refresh a color screen while the total no. of bits in an email may not reach even a million.

Techniques for Achieving Good QOS: These are four techniques that can be used to improve quality of service. These are as follows:

1. Traffic shaping
   1. Imp (a) Leaky Bucket algorithm.
   1. Imp (b) Token Bucket algorithm

2. Scheduling
   (a) FIFO Queuing
   (b) Priority Queuing
   (c) weighted fair Queuing

3. Admission Control

4. Resource Reservation.

Scanned with OKEN Scanner

(2) **Traffic shaping**: Traffic shaping is a mechanism to control the amount and the rate of the traffic sent to the network. Two techniques can shape traffic) Leaky Bucket, Token Bucket:

(a) **Leaky Bucket**: Leaky bucket is a Bucket with a hole at bottom. Flow of the water from bucket is at a constant rate which is independent of water entering the bucket. If Bucket is full, any additional water in the Bucket is thrown out.

(Same) / Same Technique is applied to control congestion in network traffic. Every host in the network is having a buffer with finite queue length. Packets which are put in the buffer when buffer is full are thrown away.

"A Leaky Bucket algorithm shapes bursty traffic into fixed rate traffic by averaging the data rate. It may drop the packets if the bucket is full".

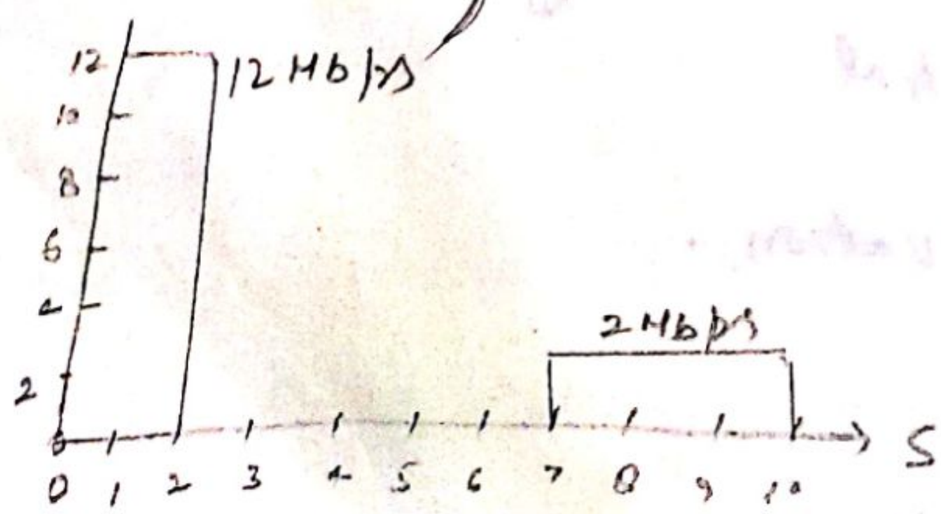


fig: Bursty data

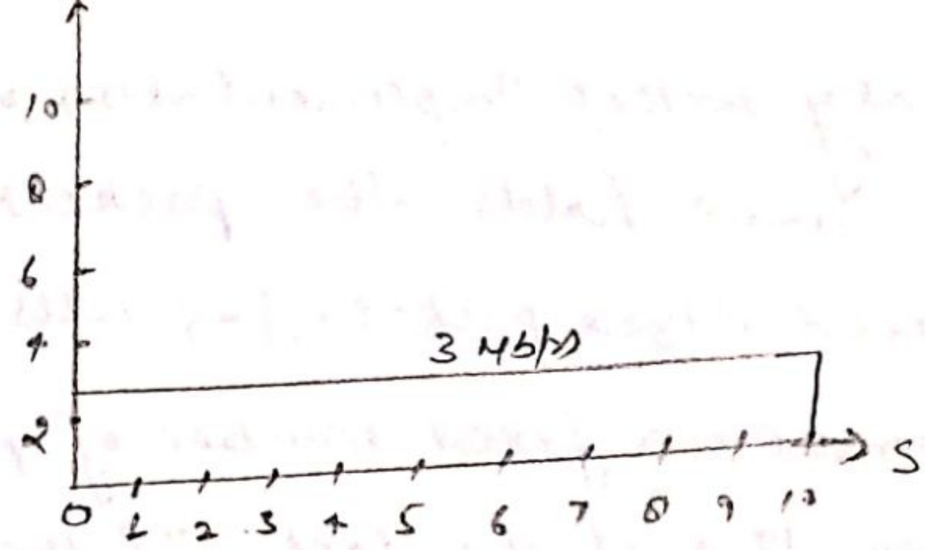


fig: Fixed Rate data

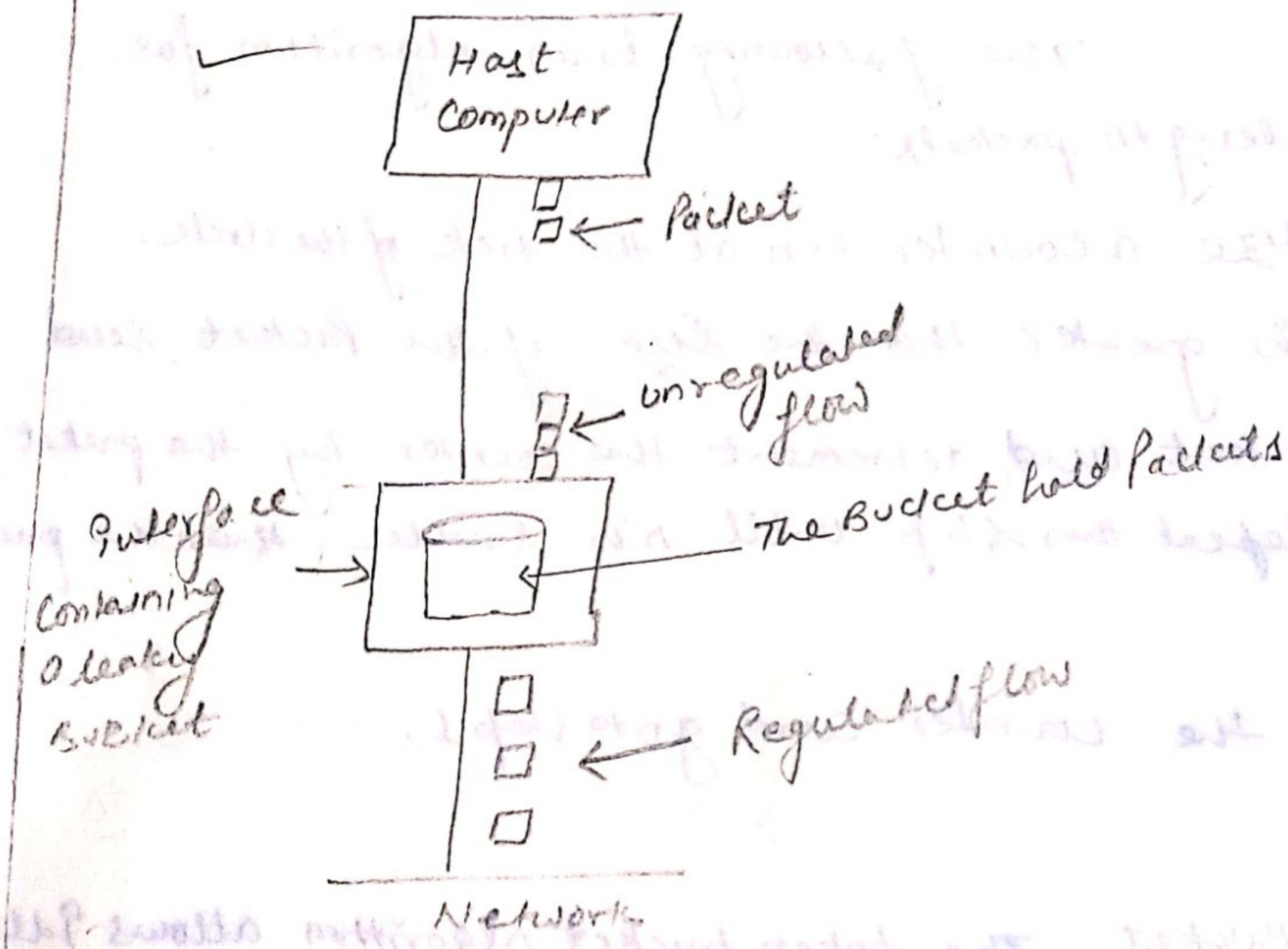


fig. Leaky Bucket algorithm

Leaky Bucket Implementation:

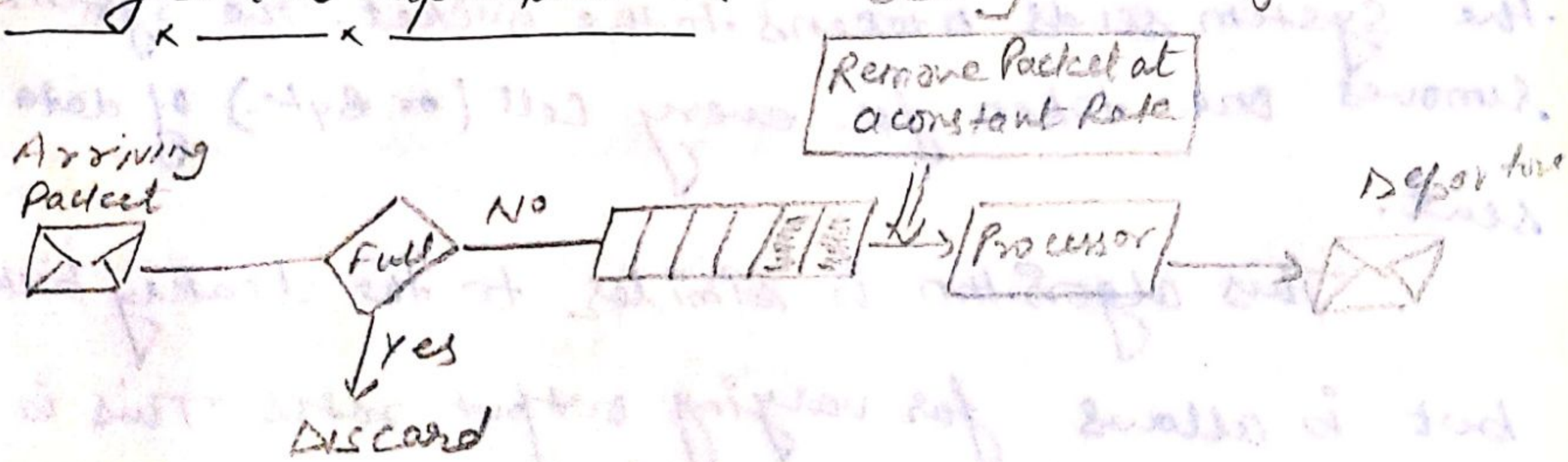


fig 4.30

A simple leaky bucket implementation is shown in fig: 4.38. A FIFO queue holds the packets. If the traffic consists of fixed sized packets (eg. cells in ATM N/W) the process removes a fixed number of packets from the queue at each tick of the clock. If the traffic consists of variable-length packets, the fixed output rate must be based on the number of bytes or bits.

The following is an algorithm for variable length packets:

1: Initialize a counter to n at the tick of the clock.

2: If n is greater than the size of the packet, send the packet and decrement the counter by the packet size. Repeat this step until n is smaller than the packet size.

3. Reset the counter and go to step 1.

(B) Token Bucket: (The token bucket algorithm allows idle hosts to accumulate credit for the future in the form of tokens. (In token Bucket For each tick of the clock, the system sends n tokens to the bucket. The system removes one token for every cell (or byte) of data sent.)

(This algorithm is similar to the leaky bucket but is allows for varying output rates. This is useful when larger burst of traffic arrive).

Scanned with OKEN Scanner

→ It enforces a long-term average transmission rate while permitting bounded bursts. In this approach, a token bucket is used to manage the queue regulator that controls the rate of packet flow into the network.

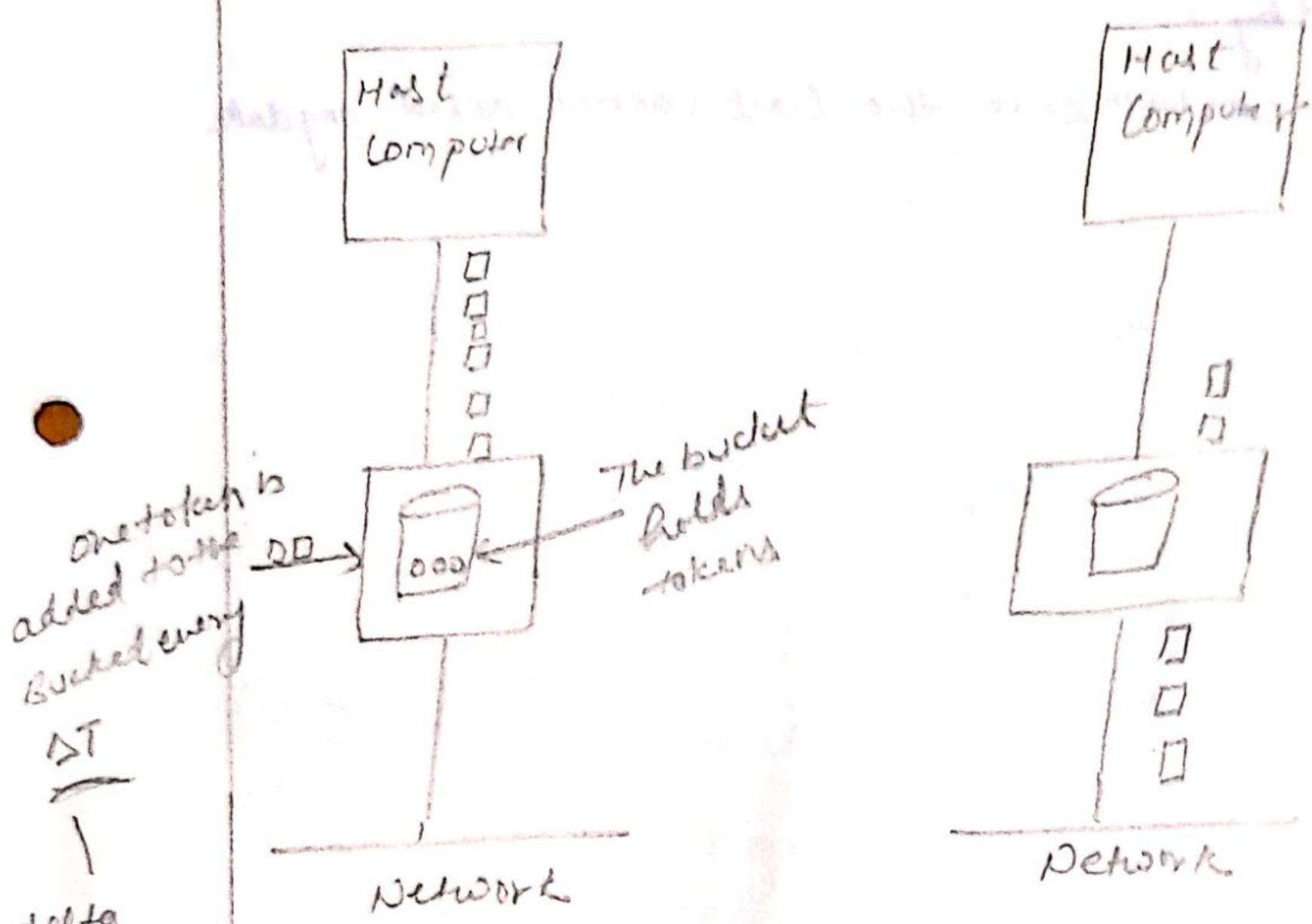


fig Token Bucket algorithm

→ A token generator constantly produces tokens at a rate of R tokens per second and places them into a token bucket with a depth of D tokens.

→ Assuming that each token grants the ability to transmit a fixed number of bytes, if the token bucket fills, newly generated tokens are discarded.

Implementation of token bucket:

→ The Token Buket Can be easily Implemented with a counter. The token is Initialised to zero.

→ Each time a token is added, the counter Incremented by 1 and each time a unit of data is dispatched, the counter is decremented by 1.

→ If the counter contain zero, the host Cannot send any data.

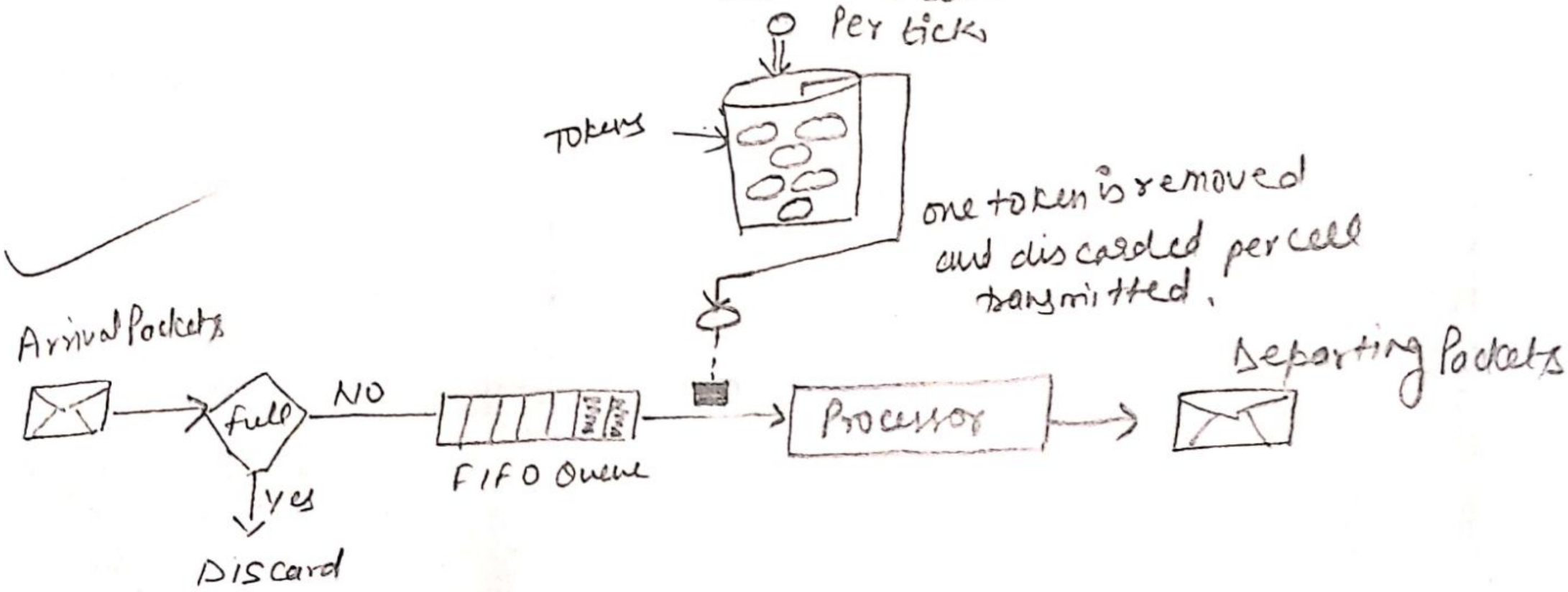


fig Implementation of Token Bucket

Note " The token Bucket allows the Bursty traffic at maximum possible rate.

Token Bucket Performance:

Let, S = Burst length (seconds)

C = bucket Capacity (Bytes)

P = token arrival rate (Bytes/second)

& m = maximum source rate (Byte/second)

What is the duration of a maximum-rate Burst through a token Bucket?

(i) maximum Bytes sent from the token Bucket during a Burst is

$$C + p \cdot s$$

(ii) Maximum Bytes the source can send during a Burst is

$$m \cdot s$$

(II) Setting the two equal & solving for s

$$\boxed{s = \frac{C}{m-p}}$$

or

$$C + p \cdot s = m \cdot s$$

$$C = m \cdot s - p \cdot s$$

$$C = s(m-p)$$

$$\boxed{\text{then } s = \frac{C}{(m-p)}}$$

(2.) <u>Scheduling</u>: Packets from different flows arrive at a switch or router for processing. A good scheduling Technique treats the different flows in a fair and appropriate way (manner). Several scheduling Techniques are designed to improve the quality of service.

(A) <u>FIFO Queuing</u>: In first-in, first out (FIFO) queuing, packets wait in a Buffer (queue) until the node (router or switch) is ready to process them. If the average arrival rate is higher than the average processing rate, the queue will fill up and new packets will be discarded. A FIFO queue is familiar

Scanned with OKEN Scanner

to those who have had to wait for a Bus at a Bus stop.

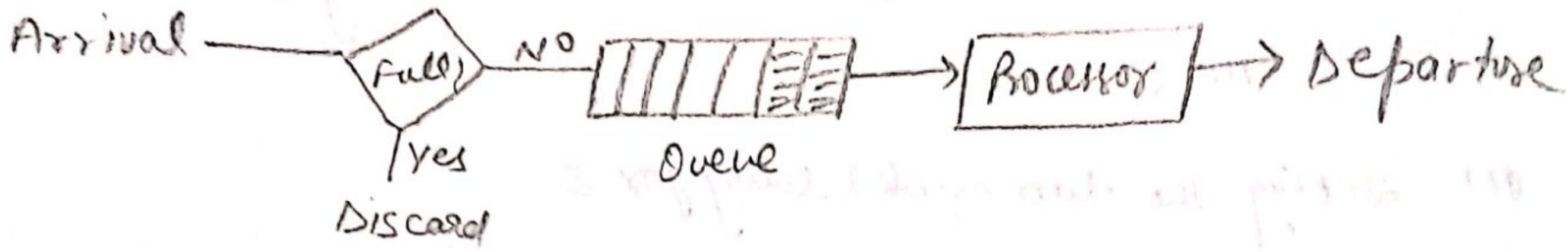


fig FIFO queue

(B) Priority Queuing: In Priority queuing, packets are first assigned to a priority class. Each priority Class has ito own queue. The packets in the highest-priority queue are processed first. packets in the lowest-priority queue are processed last. Note that the system does not stop serving a queue until it is empty.

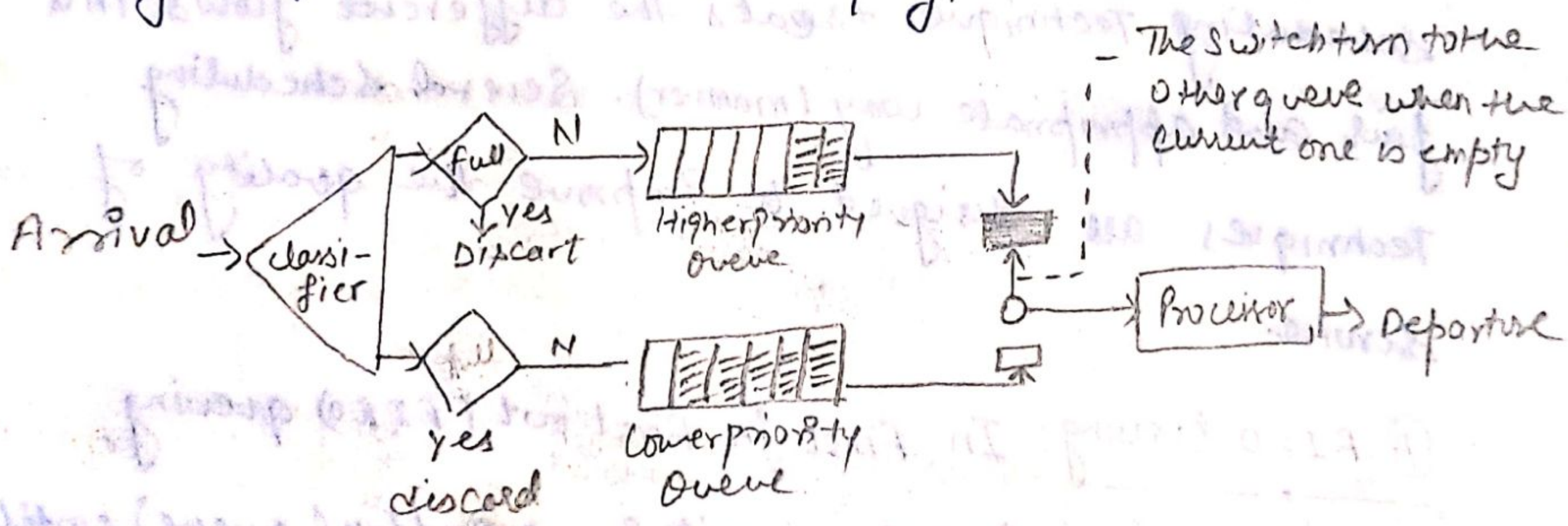


fig: Priority queuing

A priority queue can provide better quality of service (QOS) than the FIFO queue, because higher priority

traffic, such as multimedia, can reach the destination with less delay. However there is a potential drawback. If there is a continious flow in a high-priority queue the packets in the lower priority queues will never have a chance to be processed. This is a condition called starvation.

(c) Weighted fair ~~Queue~~ Queuing: A better scheduling method is weighted fair queuing. In this technique, the packets are still assigned to different classes and admitted to different queues. The queues, however, are weighted based on the priority of the queues; higher priority means a higher weight. The system processes packets in each queue in a Round-Robin fashion with the no. of packets selected from each queue based on the corresponding weight.

The turning switch selects
3 packets from first queue, then
2 " from second queue, then
1 packet from the third queue
the cycle repeats.

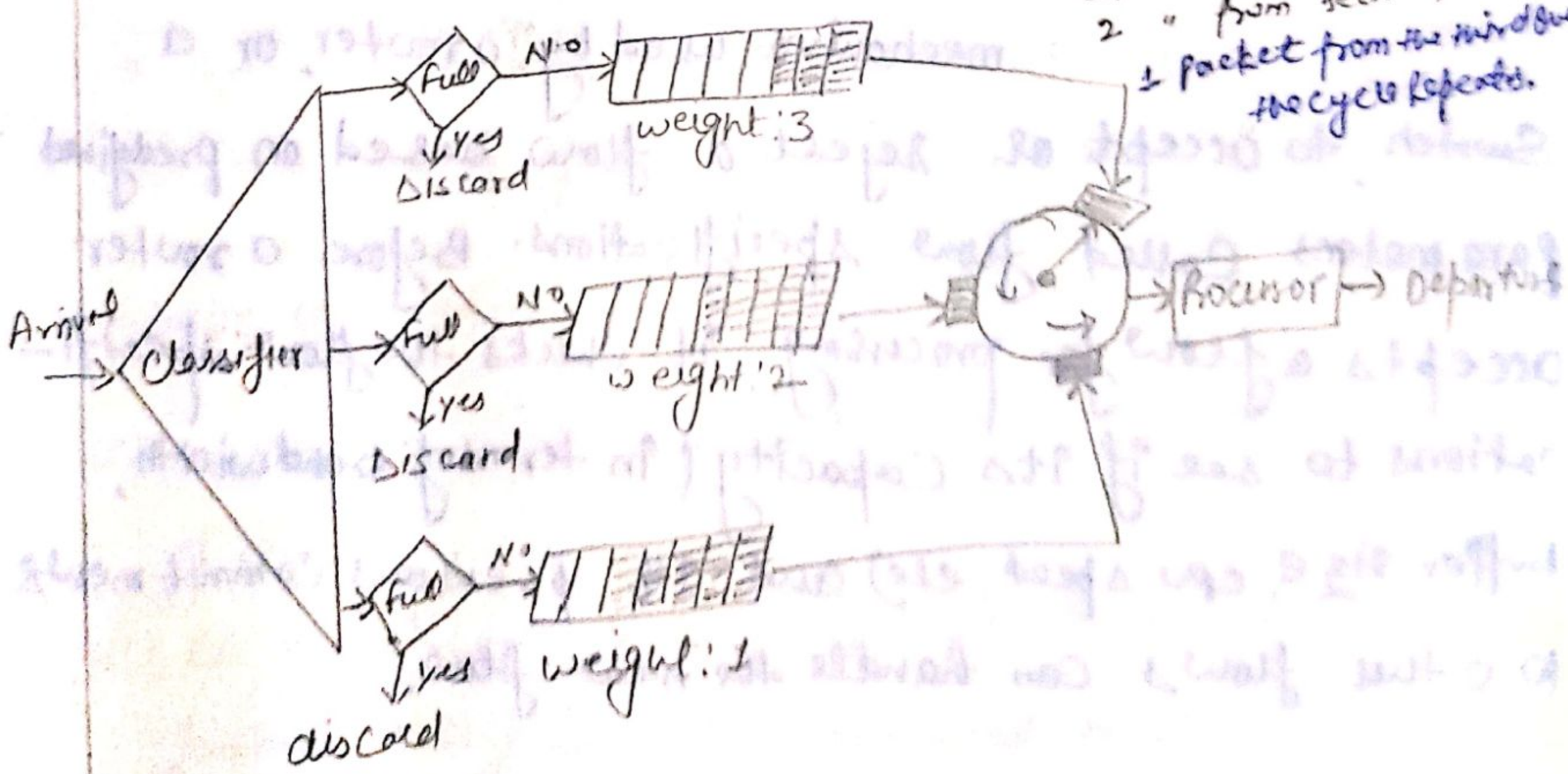


fig: weighted fair queuing

For example: If the weights are 3, 2 and 1, three packets are processed from the first queue, two from the second queue and one from the third queue. If the system does not impose priority on the classes, all weights can be equal. In this way, we have fair queuing with priority.

③ Resource Reservation:- A flow of data needs resources such as a buffer, bandwidth, CPU time, and so on. The quality of service is improved if these resources are reserved beforehand. We discuss in this section one QOS model called Integrated Services, which depends heavily on resource reservation to improve the quality of service.

④ Admission Control:- Admission control refers to the mechanism used by a router, or a switch, to accept or reject a flow based on predefined parameters called flow specifications. Before a router accepts a flow for processing, it checks the flow specifications to see if its capacity (in terms of bandwidth, buffer size, CPU speed, etc) and its previous commitments to other flows can handle the new flow.

Scanned with OKEN Scanner

Imp

Tunneling :- A Technique of internetworking called tunneling is used when source and destinations networks of same type are to be connected through a network of different type. For example, An Ethernet to be connected to another Ethernet through a WAN.

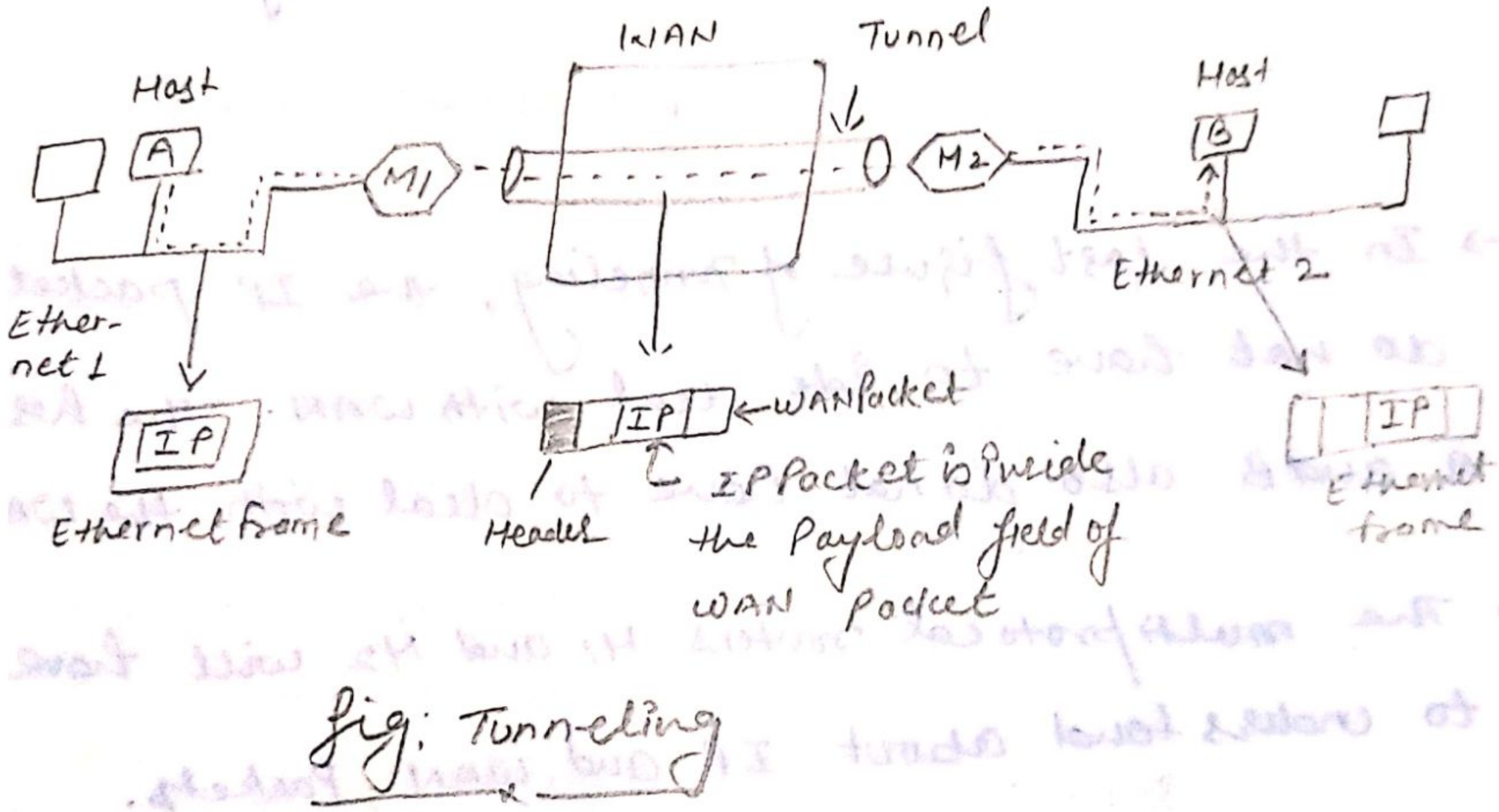


fig: Tunneling

→ The task is send an IP packet from Host A of Ethernet 1 to the Host B of Ethernet 2 via a WAN.

Sequence of Events:

i) Host A Constructs a packet containing the IP address of Host B.

ii) It then inserts this IP Packet into an Ethernet frame. This frame is addressed to the multiprotocol router M1.

(iii) Host A then puts this frame on Ethernet.

(iv) When M_1 receives this frame, it removes the IP packet, inserts it in the payload packet of the WAN network layer packet and addresses the WAN packet to M_2.

The multiprotocol Router M_2 removes the IP packet and sends it to host B in an Ethernet frame.

Why is this Technique Called tunneling?

→ In the last figure of Tunneling, the IP packets do not have to ~~ide~~ deal with WAN. The host A and B also do not have to deal with the WAN.

→ The multiprotocol routers M_1 and M_2 will have to understand about IP and WAN Packets.

→ So the WAN can be imagined to be equivalent to a big tunnel extending between the multi-protocol routers M_1 and M_2 and the technique is called as tunneling.

$\frac{1000}{5} = 200$

$1000000 \div 5 = 200000$

200000

Numericals :-

(1) An ATM network uses a token bucket scheme for traffic shaping. A new token is put into bucket every 5 ms. What is the maximum sustainable net data rate (excluding the header bit)?

1 microsec $= 10^{-6}$ sec.

Solⁿ: given net token is put every 5 ms.

maximum output datarate $m = ?$

the token arrival rate $p = \frac{1}{5\,ms} = \frac{1}{5 \times 10^{-6}} = 200\,kbps.$

$\Rightarrow \frac{1,00,000}{5} = 2,00,000\,bps = 200\,kbps$

the maximum output rate can be obtained from the following expression.

$$C = S(m-p)$$

$= C = Sm - Sp$

$+Sm = Sp + C$

$m = \frac{Sp + C}{S}$

$m = \frac{C}{S} + P$

where C = bucket capacity

M = Maximum output rate

P = token arrival rate

S = time for which the maximum output is obtained

$$\therefore \quad m = \frac{C}{S} + P$$

Assume $C = 1\,Mb/s$ and $S = 20$ ms. target

$$m = \frac{1 \times 10^{6}}{20 \times 10^{-3}} + (200 \times 10^{3})$$

$$m = 50.2\ mb/s$$ Ans

(2) A Computer on a 6-mbps network is regulated by token bucket. Token bucket filled at a rate of 1 Mbps. It is initially filled to a capacity with 8 megabits. How long can computer transmit at the full 6 ~~mp~~ Mbps?

Sol^n:

Given c = Bucket capacity = 8 Mbits

m = maximum output rate = 6 Mbps.

p = token arrival rate = 1 Mbps.

Find s = Time for which maximum output is obtained.

$$S = \frac{c}{m-p}$$

$$= \frac{8 \text{ mbits}}{6 \text{ Mbps} - 1 \text{ mbps}}$$

$$= \frac{8 \text{ mb}}{5 \text{ mb}}$$

$$\boxed{S = 1.6 \text{ sec}}$$

So the Computer can transmit at the full 6 Mbps for 1.6 second. Ans