- In CDMA the users access the channel in a random manner. Hence the signals transmitted by multiple users will completely overlap both in time and in frequency.

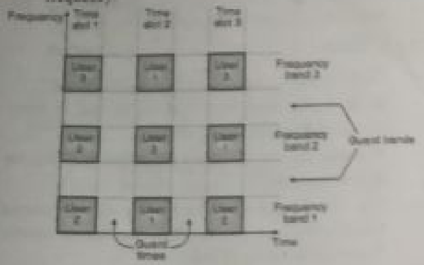


Fig. 9.7.3 : Structure of CDMA showing the guard bands and the guard times

- The CDMA signals are spread in frequency. Therefore the demodulation and separation of these signals at the receiver can be achieved by using the pseudorandom code sequence. CDMA is sometimes also called as Spread Spectrum Multiple Access (SSMA).
- In CDMA as the bandwidth as well as time of the channel is being shared by the users, it is necessary to introduce the guard times and guard bands as shown in Fig. 9.7.3.
- CDMA does not need any synchronization, but the code sequences or signature waveforms are required to be used.

9.7.4 Comparison of FDMA, TDMA and CDMA :

Sr. No.	FDMA	TDMA	CDMA
1.	Overall bandwidth is shared among many stations.	Time sharing takes place.	Sharing of bandwidth and time both takes place.
2.	Due to nonlinearity of devices inter modulation products are generated due to interference between adjacent channels.	Due to incorrect synchronization there can be an interference between the adjacent time slots.	Both type of interferences will be present.
3.	Synchronization is not necessary.	Synchronization is essential.	Synchronization is not necessary.
4.	Code word is not required.	Code word is not required.	Code words are required.
5.	Guard bands between adjacent channels are necessary.	Guard times between adjacent time slots are necessary.	Guard bands and Guard times both are necessary.

Review Questions

Q. 1 Explain the layered architecture of LAN explaining the function of the LLC and MAC sublayer.

Q. 2 What is static and dynamic channel allocation ?

Q. 3 Compare and explain the pure and slotted ALOHA system.

Q. 4 Explain the different CSMA protocols.

Q. 5 What is CSMA with collision detection ?

Q. 6 Explain the FDDI system.

Q. 7 What are the functions of a transceiver ?

Q. 8 Why there is no need of CSMA/CD for a full duplex Ethernet LAN ?

Q. 9 Explain CSMA/CD.

Q. 10 What is CSMA/CA ?

□□□

CHAPTER 10

Unit III

Connecting Devices & Virtual LANs

Syllabus :
Connecting devices and virtual LANs, Connecting devices, Hubs, Link layer switches, Routers.

10.1 Network Connecting Devices :

- Different types of network connecting devices are as shown in Fig. 10.1.1.

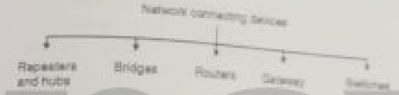


Fig. 10.1.1

- The relation between OSI reference model and various connecting devices is shown in Fig. 10.1.2.

Network connecting devices :

- Two or more devices are connected to each other for the purpose of sharing data or resources from a network.
- A LAN may be spread over a larger distance than its media can handle effectively. The number of stations also can be more than a number which can be handled and managed properly. Such networks should be subdivided into smaller networks and these smaller subnetworks should be connected to each other through connecting devices.
- A device called a repeater is inserted into the network to increase the coverable distance or a device called a bridge can be inserted for traffic management.
- When two or more separate networks are connected for exchanging data or resources it creates an internetwork. Routers and gateways are used for internetworking.
- Each of these device type interacts with protocols at different layers of the OSI model.
- Repeaters act only upon the electrical components of a signal and are therefore active only at the physical layer.
- Bridges utilize addressing protocols and can affect the flow control of a single LAN. Bridges are most active at the data link layer.
- Routers provide links between two separate but same type LANs and are active at the network layer.
- Finally gateways provide translation services between incompatible LANs or applications and are active in all of the layers. Connecting devices and the OSI model is shown in Fig. 10.1.2.

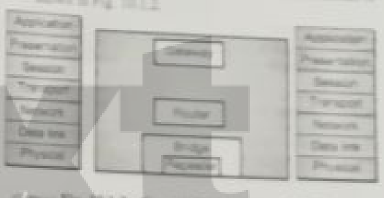


Fig. 10.1.2 : Connecting devices and OSI model

Categories of connecting devices

Fig. 10.1.2 shows the relationship between the connecting devices and various layers of the internet model.

Table 10.1.1 : Role of networking devices

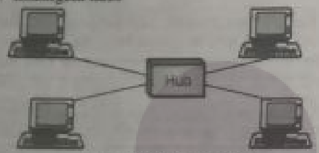
Sr. No.	Name of the device	Role
1.	Passive hub	Operate below the physical layer.
2.	Repeater	Regenerates the original signal. Operates in the physical layer.
3.	Bridge	Bridges utilize the address protocol. They can carry out the traffic management. They are most active in the data link layer.
4.	Routers	Routers provide connections between two separate but compatible networks. It works in the network layer.
5.	Gateways	Gateways provide translation services between incompatible networks and works in all the layers.

10.2 Hubs :

- The general meaning of the word hub is any connecting device. But its specific meaning is multiport repeater.
- It is normally used for connecting stations in a physical star topology.
- All networks require a central location to connect various segments of media coming from various nodes.
- Such a central location is called as a hub. A hub organises the cables and relays signals to the other media segments as shown in Fig. 10.2.1.
- There are three main types of hubs :

  1. Passive hubs 2. Active hubs

  3. Intelligent hubs



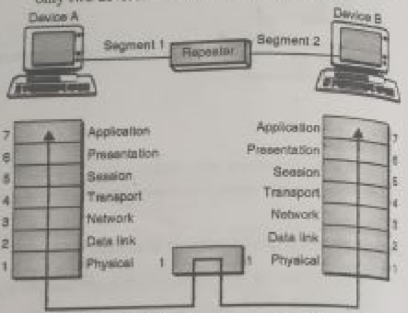
(G-350) Fig. 10.2.1 : Hub

10.2.1 Passive Hubs :

- A passive hub simply combines the signals of a network segments. There is no signal processing or regeneration. It merely acts as a connector.
- A passive hub reduces the cabling distance by half because it does not boost the signals and in fact absorbs some of the signal.
- With a passive hub, each computer receives the signals sent from all the other computers connected to the hub.
- This type of hub is a part of communication media. Hence its location is below the physical layer.

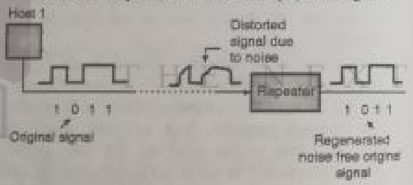
10.3 Repeaters :

- A repeater is a connecting device which can operate only in the physical layer.
- All transmission media weaken the electromagnetic waves that travel through them.
- Attenuation of signals limits the distance any medium can carry data. Devices that amplifies signals to ensure data transmission are called repeaters.
- A repeater receives a signal and before it gets attenuated or corrupted, regenerates the original signal.
- Thus we can use a repeater to extend the physical length of LAN as a shown in Fig. 10.3.1(a).
- Repeater is not an amplifier because amplifiers simply amplify the entire incoming signal along with noise.
- Signal – regenerating repeaters create an exact duplicate of incoming data by identifying it amidst the noise, reconstructing it and retransmitting only the desired information.
- The original signal is duplicated, boosted to its original strength and sent as shown in Figs. 10.3.1(a) and (b).
- A repeater does not connect two LANs. It connects only two devices connected in the same LAN.



(G-351) Fig. 10.3.1(a) : Repeater in OSI model

- It cannot connect two LANs of a different protocols.
- A repeater forwards every frame, it cannot filter out some frames and let the others pass through.
- A repeater should be placed at a precise point on the link. Such that the signal reaches it before the noise has induced an error in any of the transmitted bits.
- Fig. 10.3.1(b) illustrates the function of a repeater.
- Repeaters operate at the physical layer of the OSI model and they deal with the actual physical signals.


Host 1
Distorted signal due to noise
Repeater
1 0 1 1
Original signal
1 0 1 1
Regenerated noise free orignal signal

(G-352) Fig. 10.3.1(b) : Function of a repeater

Advantages of repeater :

1. Repeaters can regenerate the desired information.
2. They can reduce the effect of noise.
3. They can extend the network.
4. It reduces the number of errors introduced due to noise.

Disadvantages of repeater :

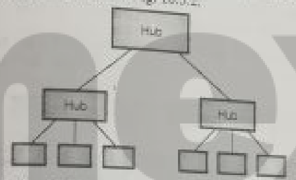
1. A repeater can not connect two LANs. It can only connect two devices connected in the same LAN.
2. It has no filtering capability.
3. Repeaters can operate only in the physical layer.
4. Repeaters must be placed at the precise point on the link so as to be effective.

10.3.1 Active Hubs :

- They are like passive hubs but have electronic components for regeneration and amplification of signals. By using active hubs the distance between devices can be increased. An active hub is equivalent to a multipoint repeater.
- The main drawback of active hubs is that they amplify noise as well along with the signals. They are more expensive than passive hubs as well.

10.3.2 Intelligent Hubs :

- In addition to signal regeneration, intelligent hubs perform some other intelligent functions such as network management and intelligent path selection.
- A switching hub chooses only the port of the device where the signal needs to go, rather than sending the signal along all paths.
- Hubs can also be used to create multiple levels of hierarchy as shown in Fig. 10.3.2.



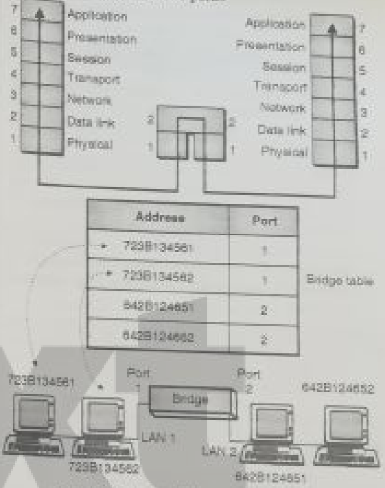
(L-446) Fig. 10.3.2 : Hubs to create multiple levels of hierarchy

10.4 Bridges :

- A bridge can operate in the physical layer as well as in the data link layer of the OSI model.
- It can regenerate the signal that it receives and it can check the physical (MAC) addresses of source and destination mentioned in the header of a frame.

Filtering :

- The major difference between the bridge and repeater is that the bridge has a filtering capability. That means a bridge will check the destination address of a frame and make a decision about whether the frame should be forwarded or dropped.
- If the frame is to be forwarded, then the bridge should specify the port over which it should be forwarded.
- In order to achieve this a bridge has a table relating the addresses and ports as shown in Fig. 10.4.1.
- If a frame for 723B134561 arrives at port 2 then the bridge goes through its table and understands that the frame is to be sent out on port 1 so it will do so.
- In Fig. 10.4.1 a two port bridge is shown but in reality a bridge has more than two ports.



Address	Port
723B134561	1
723B134562	1
642B124651	2
642B124652	2

(G-354) Fig. 10.4.1 : Bridge and bridge table

- It is important to note that the bridges do not change the physical address contained in the frame.

Types of bridges :

- The bridges are of two types :

  1. Transparent bridges and
  2. Routing bridges.

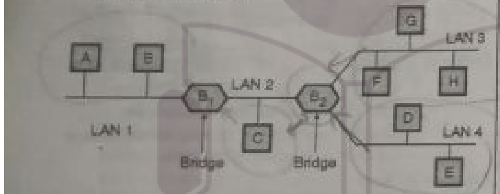
- Transparent bridge is a bridge in which the stations are not at all aware of the existence of the bridge.
- Transparent bridges keep a table of addresses in memory to determine where to send data.
- The duties of a transparent bridge are as follows :

  1. Filtering frames
  2. Forwarding and
  3. Blocking.

- In source routing a sending station defines the bridges that should be visited by the frames.
- The addresses of these bridges are included in the frame. So a frame contains not only the source and destination address but also the bridge addresses.
- Source routing bridges are used to avoid a problem called looping. These bridges were designed for the token ring LANs. But these LANs are not very common now a days.

10.4.1 Transparent Bridge :

- A transparent bridge builds its table of station addresses on its own as it performs its bridge function. When this bridge is first installed, its table is empty.
- As it comes across each packet it looks at both the destination and source addresses.
- It checks the destination to decide where to send the packet. If it does not yet recognise the destination address it relays the packet to all of the stations on both segments.
- It uses the source address to build its table. As it reads the source address it notes which side the packet came from and associates that address with the segment to which it belongs.
- As an example, consider the configuration of Fig. 10.4.2. As shown in the Fig. 10.4.2 bridge B_1 is connected to LANs 1 and 2 and bridge B_2 is connected to LANs 2, 3 and 4.
- A frame arriving at bridge B_1 on LAN 1 destined for A can be discarded immediately because it is already on the right LAN, but a frame arriving on LAN 1 for C or F must be forwarded.



(L-648) Fig. 10.4.2 : Configuration of bridge and LAN

- When a frame arrives, a bridge must decide whether to discard or forward it, and if the latter is true, then decide on which LAN to put the frame.

Bridge learning :

- When a frame arrives at one of the ports of a bridge, it has to make a decision about forwarding the frame to another port. This decision is made based on the destination address of the frame.
- In order to make such decisions every bridge needs a table called **forwarding table** or **forwarding database**.
- This table indicates which side of the port the destination station is attached to, directly or indirectly. The format of a forwarding table is shown in Table 10.4.1.

Table 10.4.1 : Format of a forwarding table

MAC address	Port

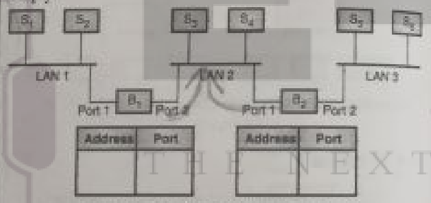
- Note that in practice there are a few thousand entries in a forwarding table.
- Let us see how to fill up these forwarding tables. It is filled up by a process called as "bridge learning".
- The basic bridge learning process is as follows :

Bridge learning procedure :

1. When a bridge receives a frame, it first compares the source address of the frame with each entry in the forwarding table. If no match is found, then the bridge will add this source address alongwith the port number on which the frame was received, to the forwarding table.
2. The bridge compares the destination address of the received frame with each entry in the forwarding table. If a match is found, then the bridge forwards the frame to the port indicated in the entry. But if this port is same as the one on which the frame was received, then the frame is discarded. Finally if a match is not found, then the bridge will send that frame on all its ports except the one on which the frame was received.

Example on bridge learning :

Consider the network shown in Fig. 10.4.2(a). Assume that forwarding tables of both the bridges are initially empty.



(L-649) Fig. 10.4.2(a) : Example network

1. **S_2 sends a frame to S_1 :**

If S_2 sends a frame to S_1, then B_1 compares the source address of the received frame with the existing entries. So here S_2 is the sender and S_1 is destination.

But there are no entries in B_1 table. So it adds the address of S_2 in its forwarding table as shown in Fig. 10.4.2(b).

Then B_1 compares the destination address of the received frame with the existing entries. But the table is empty. So the bridge B_1 thinks of flooding the frames. But then it understands that the **destination S_1 is connected on the same port (Port 1) on which the frame has been received.**

So B_1 will note down the address of S_1 in its table and **discard the frame.** This is because bridge B_1 is not required to be used when a communication between S_1 and S_2 is to be made.

- The traffic is now completely isolated in LAN 1, and the updated bridge tables are shown in Fig. 10.4.2(b).

B_1

Address	Port
S_2	1
S_1	1

B_2

Address	Port

Fig. 10.4.2(b) : Forwarding tables after $S_2 \rightarrow S_1$

2. **S_5 transmits to S_4 :**

- The two stations correspond to two different LANs. S_5 is the sender and S_4 is the destination.
- First B_2 records the address of S_5 and port number (Port 2) because the address of S_5 is not found in its forwarding table.
- Then B_2 checks the destination address. Since there are no entries, it will add S_4 and port 1 in its table as shown in Fig. 10.4.2(c). Bridge B_2 will forward the frame to port 2 of B_1 as well as to LAN 2 where S_4 will receive it.
- When this frame arrives at port 2 of B_1 it also adds the source address i.e. S_5 and port 2 in its table as shown in Fig. 10.4.2(c).
- However the destination address (S_4) is on the same port (2) of B_1 on which it has received the frame. So it will note down S_4 and port 2 in its table but **discard** the frame.

B_1

	Address	Port
$S_2 \rightarrow S_1$	S_2	1
	S_1	1
$S_5 \rightarrow S_4$	S_5	2
	S_4	2

B_2

	Address	Port
$S_5 \rightarrow S_4$	S_5	2
	S_4	1

Fig. 10.4.2(c) : Forwarding tables after $S_5 \rightarrow S_4$

- The table entries for the remaining transmissions are given in Figs. [illegible] and (e).

3. **S_3 transmits to S_5 :**

B_1

	Address	Port
$S_2 \rightarrow S_1$	S_2	1
	S_1	1
$S_5 \rightarrow S_4$	S_5	2
	S_4	2
$S_3 \rightarrow S_5$	S_3	2

B_2

Address	Port	
S_5	2	$S_5 \rightarrow S_4$
S_4	1	
S_3	2	$S_3 \rightarrow S_5$

Fig. 10.4.2(d) : Tables after $S_3 \rightarrow S_5$

4. **S_1 transmits to S_2 :**

No change in the tables.

5. **S_6 transmits to S_5 :**

B_1

	Address	Port
$S_2 \rightarrow S_1$	S_2	1
	S_1	1
$S_5 \rightarrow S_4$	S_5	2
	S_4	2
$S_3 \rightarrow S_5$	S_3	2

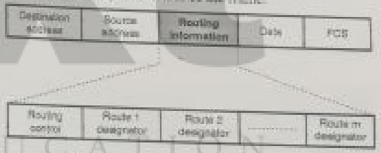
B_2

Address	Port	
S_5	2	$S_5 \rightarrow S_4$
S_4	1	
S_3	2	$S_3 \rightarrow S_5$
S_6	2	$S_6 \rightarrow S_5$

Fig. 10.4.2(e) : Table after $S_6 \rightarrow S_5$

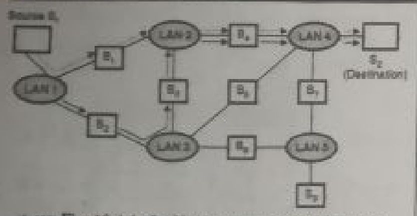
10.4.2 Source Routing Bridges :

- The source routing bridges were developed by the IEEE 802.5 committee and they are used basically to interconnect token ring networks.
- The main idea of source routing is that each station should determine the route to the destination when it wants to send a frame and therefore include the route information in the header of the frame.



(L-664) Fig. 10.4.3 : Frame format for source routing

- The frame format for source routing is shown in Fig. 10.4.3.
- Note that the routing information field is inserted only if the two communicating stations are on different LANs.
- Fig. 10.4.4 shows the LAN interconnection with source routing bridges. If station-1 wants to send a frame to station-2 then a possible route can be LAN-1 → B_1 → LAN 2 → B_4 → LAN 4.
- Many more routes are available for the same source destination pair.
- In general when a station wants to transmit a frame to another station on a different LAN, the station consults its routing table.
- If the route to the destination is found, then the station simply inserts the routing information into the frame.



(L-488) Fig. 10.4.4 : LANs interconnected with source routing bridges

How to discover a route ?

To discover a route the basic idea is as follows :

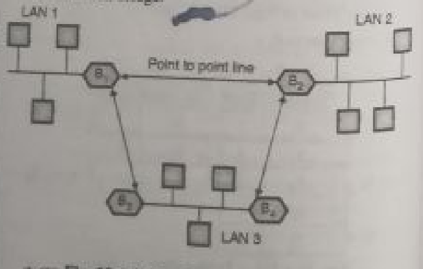
1. The station who wants to discover a route first broadcasts a special frame called single route broadcast frame.
2. This frame will visit every LAN exactly once and eventually reaches the destination.
3. Then the destination station responds with another special frame called the all routes special frame which generates all possible routes back to the source station.
4. After collecting all routes the source chooses the best possible route and saves it.

10.4.3 Comparison of Transparent and Source Routing Bridge :

Sr. No.	Parameters	Transparent bridge	Source routing bridge
1.	Ability to reconfigure	High. Bridges keep information on location of stations.	High. Each station must learn the route to its destination before sending.
2.	Stations responsibilities	None. They just send the frames and let the bridges do the work.	They determine and maintain addresses.
3.	Bridges requirements	Routing tables and the ability to both update them and execute a spanning tree algorithm.	Ability to broadcast or forward, depending on routing designators and ability to execute a spanning tree algorithm.
4.	Routes used	Always along the spanning tree, but not necessarily the cheapest.	Stations can choose the cheapest routes to one another.
5.	Dependence on topology	None. Bridges learn where stations are relative to their ports dynamically and stations have no need to know.	Some Bridges respond to routing information and spanning tree algorithms, but stations must determine a route to a destination.
6.	Orientation	Connectionless	Connection-oriented
7.	Configuration	Automatic	Manual
8.	Failures	Handled by the bridge	Handled by the host
9.	Complexity	In the bridge	In the hosts.

10.4.4 Remote Bridges :

- If bridges are used to connect LANs, having large distance between them they are called remote bridges. Many point to point links can be used to connect these bridges as shown in the Fig. 10.4.5.
- Various protocols can be used on these point to point lines. One of them is to use a point to point data link protocol (PPP), putting complete MAC frames in the payload field.
- Another option is to strip off the MAC header and trailer at the source bridge and put what is left in the payload of the point to point protocol. A new MAC header and trailer can then be generated at the destination bridge.



(L-489) Fig. 10.4.5 : Configuration of remote bridges

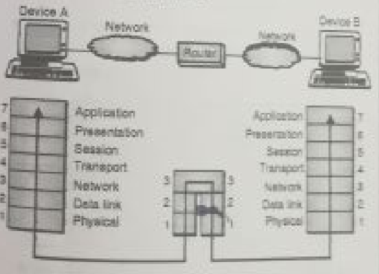
10.4.5 Bridges Connecting Different LANs :

Ideally a bridge should be able to connect LANs that use different protocols at the data link layer. For example, wired LAN and wireless LAN. But in practice the following issues are needed to be considered.

1. Frame format	2. Maximum data size
3. Bit order	4. Data rate
5. Security issues	6. Multimedia support

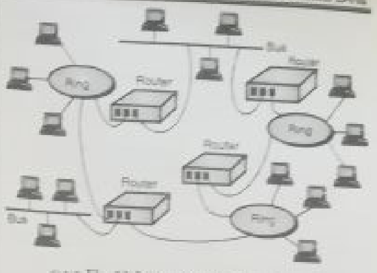
10.5 Routers :

- Routers are devices that connect two or more networks as shown in Figs. 10.5.1(a) and (b). They consist of a combination of hardware and software.
- The hardware can be in the form of a network server, a separate computer or a special device, as well as the physical interfaces to the various networks in the internetwork.
- Various types of networks can be interconnected through routers as shown in Fig. 10.5.1(b).
- The software in a router are the operating system and the routing protocol. Management software can also be used.
- Routers use logical and physical addressing to connect two or more logically separate networks.
- The large network is organized into small network segments called as subnets and these subnets are interconnected via routers.



(G-364) Fig. 10.5.1 (a) : A router in the OSI model

- Each of the subnet is given a logical address. This allows the networks to be separate but still access each other and exchange data.
- Data is grouped into packets, or blocks of data. Each packet has a physical device address as well as logical network address.
- The network address allows routers to calculate the optimal path to a workstation or computer.



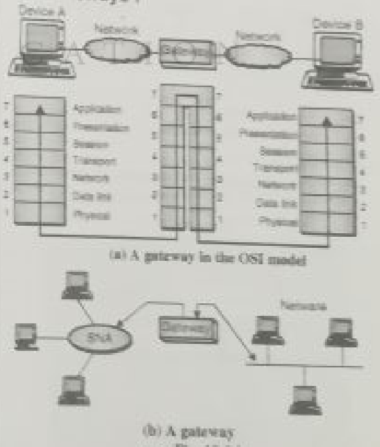
(G-365) Fig. 10.5.1(b) : Routers in an Internet

- Route discovery is the process of finding the possible routes through the internetwork and then building routing tables to store that information. The two methods of route discovery are :
  1. Distance vector routing
  2. Link state routing

Note :

- Routers work at the network layer of the OSI model.
- With static route selection, packets always follow a pre-determined path.

10.6 Gateways :



(a) A gateway in the OSI model

(b) A gateway

(G-366) Fig. 10.6.1

- 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.

- A gateway is a device that can interpret and translate the different protocols that are used on two distinct networks as shown in Figs. 10.6.1(a) and (b).
- Gateways comprise of software, dedicated hardware or a combination of both. Gateway operate through all the seven layers of the OSI model and all five layers of the internet model.
- A gateway can actually convert data so that it works with an application on a computer on the other side of the gateway. For e.g. a gateway can receive e-mail message in one format and convert them into another format.
- Gateways can connect systems with different communication protocols, languages and architecture. For e.g. IBM networks using Systems Network Architecture (SNA) can be connected to LANs using a gateway.

Note : Gateways are slow because they need to perform intensive conversions.

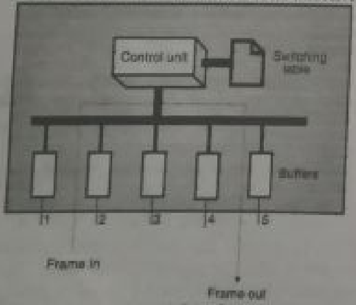
10.7 Switches :

- A switch is a device which provides bridging functionality with greater efficiency. A switch acts as a multiport bridge to connect devices or segments in a LAN.
- The switch has a buffer for each link to which it is connected. When it receives a packet, it stores the packet in the buffer of the receiving link and checks the address to find the outgoing link.
- If the outgoing link is free, the switch sends the frame to that particular link.

Switches are of two types :

1. Store - and - forward switch
2. ·Cut - through switch.

- A store - and - forward switch stores the frame in the input buffer until the whole packet has arrived.
- A cut-through switch, forwards the packet to the output buffer as soon as the destination address is received.



(G-367) **Fig. 10.7.1 : Switch**

- Concept of a switch is shown in Fig. 10.7.1. As shown in the Fig. 10.7.1 a frame arrives at port 2 and is stored in the buffer.
- The CPU and the control unit, using the information in the frame consult the switching table to find the output port. The frame is then sent to port 5 for transmission.

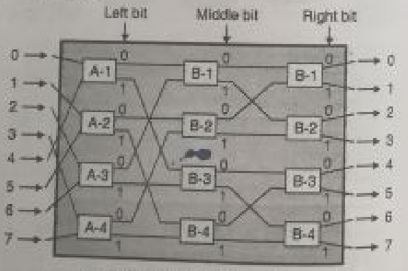
Note : Routing switches use the network layer destination address to find the output link to which the packet should be forwarded.

10.7.1 Two Layer Switch :

- The switches can be of two types namely the two layer switches and the three layer switches.
- A two layer switch operates at the physical as well as data link layer.
- The two layer switch is basically a bridge. It has many ports and it is designed to allow better performance.
- A bridge with few ports is used for connecting a few LANs together. But a bridge with many can allocate a unique port to each station. Thus each station will have its own separate identity.
- Therefore there is no competing traffic and so there are no collisions.

10.7.2 Three Layer Switch :

- A three layer switch is used at the network layer and it is a kind of router.
- A three layer switch is shown in Fig. 10.7.2.
- It has n = 8 inputs and same number of outputs. A three bit number is used to decide the internal path over which the input is passed to output.
- The number of microswitches at each stage is n/2 i.e. 4 switches.



(G-368) **Fig. 10.7.2 : A three layer switch**

- The first stage routes the cell based on the high order bit in the binary bit string.
- The second stage routes the cell based on the middle bit and last stage routes it based on the low order bit.
- Note that number of stages = $\log_2 (n) = \log_2 8 = 3$.

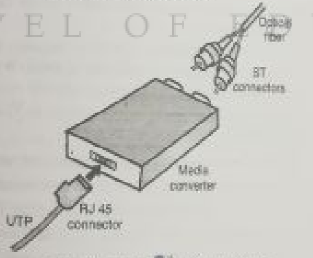
10.7.3 Comparison of Hub and Switch :

Sr. No.	Hub	Switch
1.	It is a broadcast device.	It is a point to point device.
2.	It operates at physical layer.	It operates at datalink layer.
3.	It is not an intelligent device.	It is an intelligent device.
4.	It simply broadcasts the incoming packet.	It uses switching table to find the correct destination.
5.	It can not be used as a repeater.	It can be used as a repeater.
6.	Not a sophisticated device.	It is a sophisticated device.
7.	Not very costly.	Costly.

10.7.4 Media Converters :

- It is a device which is used to connect two different networking media. For example connection between a shielded cable and twisted pair can be achieved through the media converter.
- Fig. 10.7.3 shows the media converter.
- Various functions performed by a media converter are as follows :

1. Connect two different types of wiring systems without an additional repeater.



(G-369) **Fig. 10.7.3 : Media converter**

2. Connect two 10 Base T or 100 Base TX networks in different buildings using fiber-optic cable.
3. To allow the use of different types of cables such as UTP cabling, thin net fiber optic cable, thick net etc. in a single network.

10.7.5 Comparison of Router and Bridge :

Sr. No.	Parameter	Router	Bridge
1.	Layer in OSI model.	Network layer	Physical or data link.
2.	Operation.	Connect two or more network.	Regeneration, check MAC address.
3.	Types.	Distance vector, Link state	Transparent, Routing.
4.	Principle of working.	Uses hardware and software.	Uses tables relating the addresses and ports.
5.	Used for	Connecting networks	Connecting computers.

10.7.6 Comparison of Bridge, Switch and Hub :

Sr. No.	Parameter	Hub	Switch	Bridge
1.	Type of device	Broadcast	Point to point ,	Both
2.	Layer of operation	Physical	Data link	Physical and data link
3.	Intelligence	Not intelligent	Intelligent	Highly intelligent
4.	Duties	Simply broadcast the incoming packet	Uses switching table to find correct destination	Filtering, forwarding and blocking of frames
5.	Sophistication	Low	High	Very high
6.	Cost	Low cost	Expensive	Very expensive

10.7.7 Comparison of Bridges, Routers and Switches :

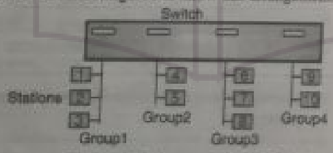
Table 10.7.1

Sr. No.	Parameter	Router	Bridge	Switch
1.	Layer in OSI model	Network layer	Physical or data link	Data link and network layer
2.	Type of device	Point to point	Point to point or broad cast	Point to point
3.	Operation	It connects two or more networks	It regenerates, checks MAC address	It provides bridging operation with greater accuracy

Sr. No.	Parameter	Router	Bridge	Switch
4.	Types	Distance vector, link state	Transparent, Routing	Two layer, three layer.
5.	Intelligence	Highly intelligent	Highly intelligent	Highly intelligent
6.	Used for	Connecting networks	Filtering forwarding and blocking frames.	Uses switching table to find correct destination.

10.8 Virtual LANs :

- The virtual local area network (VLAN) is a LAN configured not by physical wiring like conventional LAN but it is configured by software.
- It is developed in order to establish a connection between two stations belonging to two different physical LANs.
- The concept of VLAN technology is based on dividing a LAN into logical instead of physical segments. A LAN can be divided into several logical LANs called VLANs.
- The concept of VLAN will be clear after referring to Fig. 10.8.1 which shows the conventional swiched LAN.
- The total number of stations are grouped into 4 groups and the groups are connected by a switch.
- The LAN is configured to allow this arrangement.

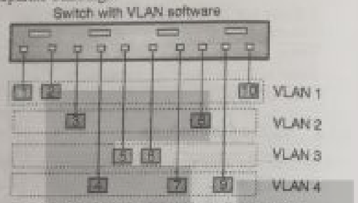


(L-744) Fig. 10.8.1 : A conventional LAN

- In a conventional LAN if we wish to transfer stations 1 and 2 from group 1 to any other group, then the LAN configuration needs to be changed. Rewiring would be required.
- This is the biggest problem in the conventional LAN. But the problem is solved by using a VLAN.

10.8.1 VLAN Configuration :

- Fig. 10.8.2 shows the configuration of VLAN connecting the same ten stations in four VLAN segments.
- The total stations are divided in four logical instead of physical segments. A LAN can be divided into several logic LANs called VLANs.
- It is possible to move one station from one group to any other group without changing the physical configuration because the membership of a group is defined by software and not by hardware.
- Any station can be moved logically to another VLAN.
- All the members corresponding to a VLAN can receive the broadcast message broadcast sent to that VLAN.
- Using the VLAN technology it is even possible to group stations connected to different switches.
- VLAN is very useful for a company having two separate buildings.



(L-745) Fig. 10.8.2 : VLAN configuration

- Thus VLANs group stations belonging to one or more physical LANs into broadcast domain. The stations in a VLAN communicate with each other as if they belong to the physical segment.

10.8.2 Membership :

- There are various characteristics used to group various stations in a VLAN.
- Some of such characteristics are port number, MAC addresses, IP addresses, IP multicast address. We can use them singly or a combination of two or more characteristics for grouping various stations in VLAN.

1. **Port number :**
   - An administrator may define that the stations connected to ports 1, 3, 5, 7 of a switch correspond to VLAN-1, the stations connecting to ports 2, 4, 6, 8 correspond to VLAN-2 etc. So in this case the port number of the switch is being used as a membership characteristic.
2. **MAC addresses :**
   - The 48 bit MAC address is used as a membership characteristics by some vendors. The stations having particular MAC addresses are grouped together to form VLAN-1. The stations having some other MAC addresses form VLAN-2 etc.
3. **IP addresses :**
   - The 32-bit IP addresses are used us membership characteristics by some vendors. The principle is same as that for the MAC addresses.

4. **Multicast IP addresses and combinations :**
   - Some vendors use the multicast IP addresses as a membership characteristics and some of them use the combination of all the characteristics mentioned earlier to form the VLANs.

10.8.3 Configurations :

The grouping of stations in a VLAN can be carried out by using one of the following configurations :

1. Manual configuration
2. Automatic configuration
3. Semiautomatic configuration

1. **Manual configuration :**
   - In the manual configuration, the network administrator assigns the stations to different VLANs using VLAN software but manually.
   - If required, the migration of a station from one VLAN to the other also takes place manually.
   - Since VLAN is a logical configuration, all the assignments and migrations take place via VLAN software.
2. **Automatic configuration :**
   - In an automatic configuration, the stations are brought into or taken out of the VLANs automatically.
   - The criteria for connection or otherwise is defined by the administrator.
3. **Semi automatic configuration :**
   - This configuration is in between the manual and automatic configurations. The initialization process is done manually whereas the migration is an automatic process.

10.8.4 Communication between Switches :

- In the backbone using multiple switches each switch is supposed to know the stations and their VLANs and the membership of stations connected to each switch.
- Methods devised for the purpose of communication between switches are as follows :
  1. Table maintenance
  2. Frame tagging.
  3. Time division multiplexing.

1. **Table maintenance :**
   - This method works in the following manner. When a station sends its broadcast frame to all the other members of its own group, the switch will create an entry in a table and note down the membership number of the broadcasting station.
   - The modified tables are sent by the switches to each other periodically for updating.
2. **Frame tagging :**
   - In this method, when a frame is moving from one switch to the other, an extra header is added to its MAC frame.
   - This extra header defines the destination VLAN. The receiving switches then use this header to determine the destination VLANs. The extra header is known as frame tag.
3. **Time division multiplexing (TDM) :**
   - In this method, the connection between switches is done on the basis of time sharing of channels which is the principle of TDM.
   - If there are six VLANs connected in a backbone network, then each trunk (connection) is divided into six channels.
   - Channel 1 is designated to VLAN-1 channel 2 to VLAN-2 and so on.

IEEE standard :

- In late 1990s the IEEE 802.1 committee passed a new standard called 802.1 Q to define the format for frame tagging.
- This standard defines the format used in multiswitched backbones as well.
- 802.1 Q is the first step towards the future standardisation and most vendors have already accepted this standard.

10.8.5 Advantages of VLANs :

Some of the advantages are :

1. Reduction in cost.
2. Saving of time required for rewiring.
3. No need to change the physical configuration.
4. VLANs provide additional security. The message broadcast in one group cannot be listened by members of other groups.

Review Questions

Q. 1 State and discuss various types of connectors.
Q. 2 What is NIC ?
Q. 3 Write a note on Transceivers.
Q. 4 Explain the function of repeaters. Is it as amplifier ?
Q. 5 Compare repeater and hub.
Q. 6 Write a note on : Bridges.
Q. 7 What is the uses of bridge table ?
Q. 8 With the help of suitable explanatory diagram, explain the routers and gateways.
Q. 9 Explain different types of switches.
Q. 10 Compare switches and hub.
Q. 11 What is backbone network ? What are its types ?
Q. 12 Explain the following : 1. Bus backbone 2. Star backbone.

❑❑❑