__/__/__

Date : 25.07.2023

Subject : Data Communication And Networking.

UNIT - 5

WIRELESS LAN

→ connecting devices without use of cables

IEEE 802.11

→ defined specifications for a wireless LAN covering physical and data link layer.

Architecture - has 2 kinds of services.

- BSS - basic service set
- ESS - extended service set.

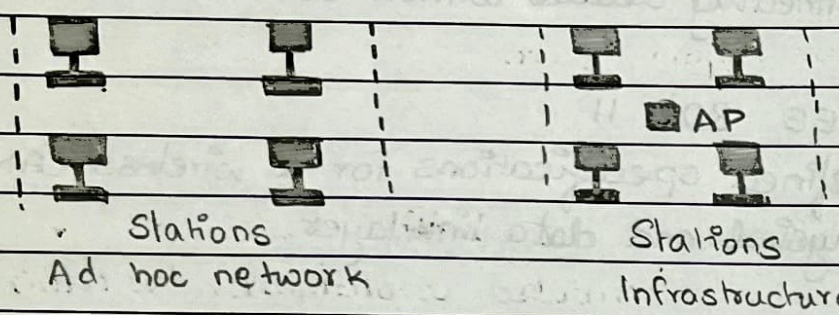
BASIC SERVICE SET

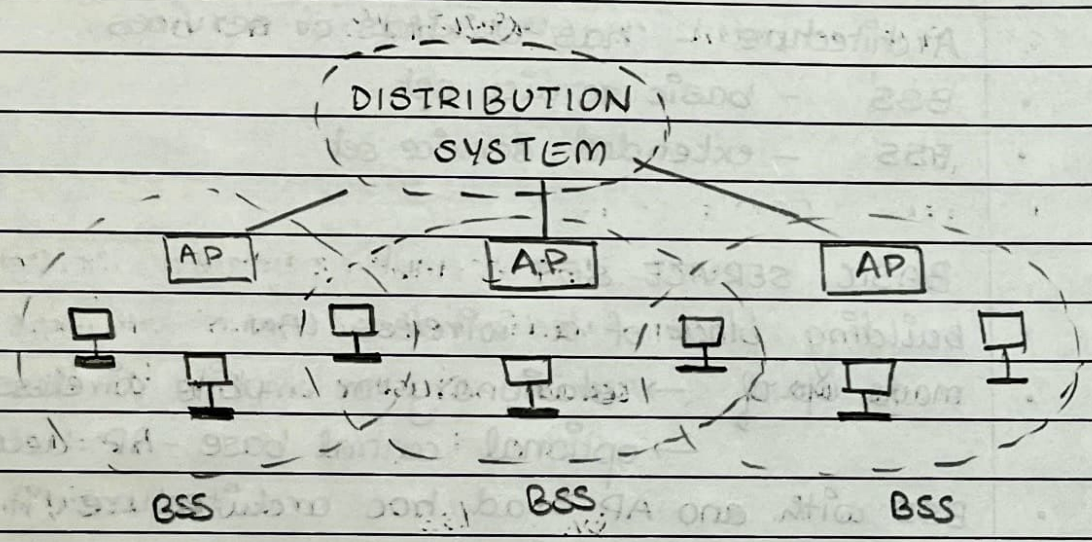
- building block of a wireless LAN.
- made up of → stationary or mobile wireless stations
  → optional central base - AP - access point.
- BSS with no AP - ad hoc architecture, it is a stand alone network, cannot send data to other BSS - stations locate each other and form a network
- BSS with an AP - infrastructure network

EXTENDED SERVICE SET

- made of two or more BSS with an AP.
- BSS connected through distribution system - it connects APs in BSS through a wired LAN.
- ESS has 2 types of stations :
  1. Mobile : normal stations inside a BSS
  2. Stationary : AP stations.

- stations within reach can communicate without an AP.
- communication b/w 2 stations which are a part of different BSS require an AP.
- mobile station can belong to more than one BSS





- TYPES OF STATIONS
  - Based on their mobility.

1. No-transition - is either stationary (not moving) or moving inside a BSS
2. BSS-transition mobility - move from one BSS to another but confined to one ESS.
3. ESS-transition mobility - move from one ESS to another.

does not gurantee communication is continuous during move.

MAC SUBLAYER

Data-link layer	→ Logical link control (LLC)	
	→ Medium Access control (MAC)	→ PCF → DCF

Physical Layer

MAC has 2 sublayers.

1. DCF - distributed co-ordination function
2. PCF - point co-ordination function.

DCF

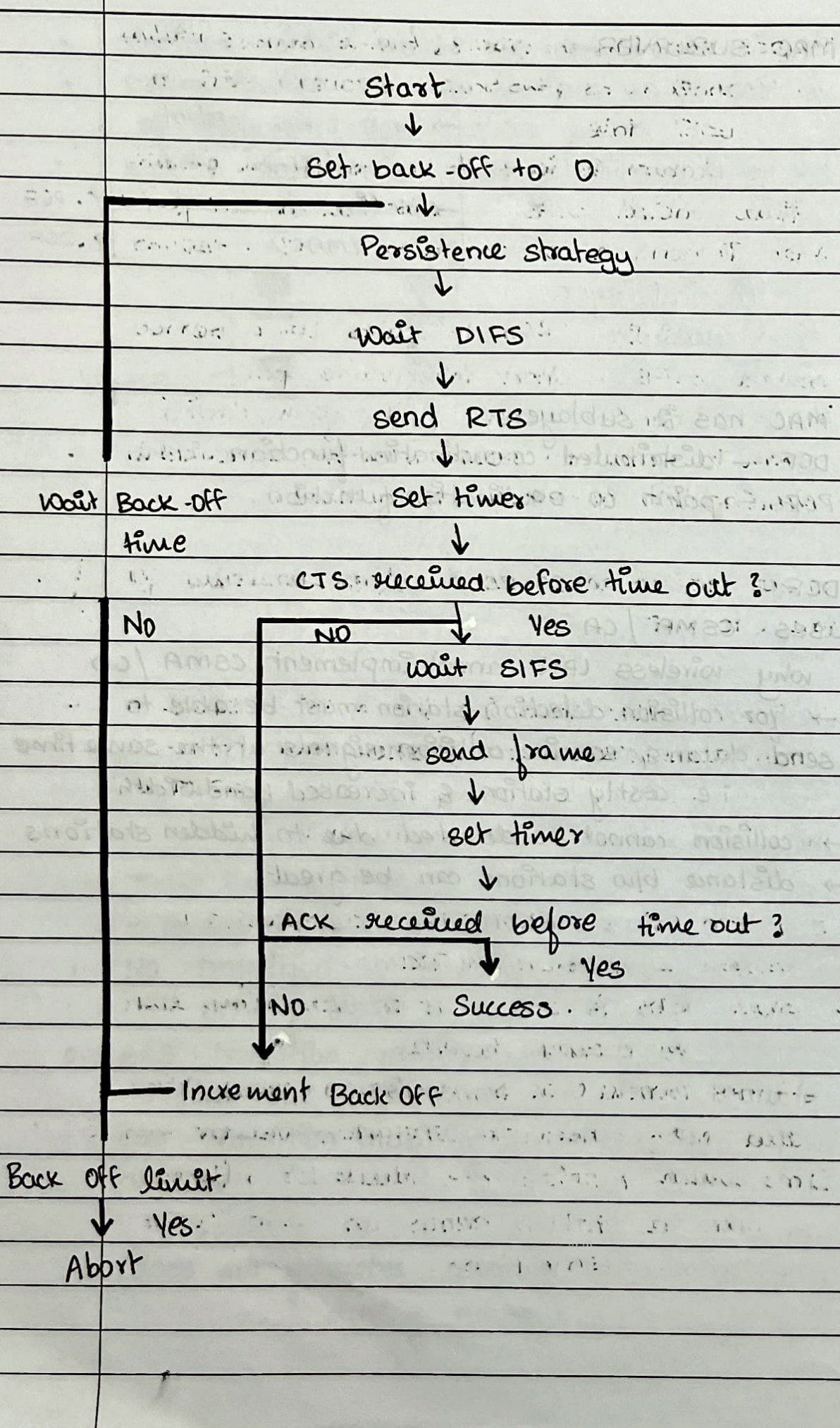
- uses CSMA / CA.

why wireless LAN cannot implement CSMA / CD

→ for collision detection station must be able to send data & receive collision signals at the same time.
i.e costly station & increased bandwidth.

→ collision cannot be detected due to hidden stations.

→ distance b/w stations can be great.


Start
Set back-off to 0
Persistence strategy
Wait DIFS
send RTS
Set timer
Wait Back-off time
CTS received before time out ?
No
NO
Yes
Wait SIFS
send frame
set timer
ACK received before time out ?
Yes
NO
Success
Increment Back Off
Back Off limit
Yes
Abort

1. Before sending a frame, source senses medium
a) channel uses persistance strategy with back-off until idle.
b) if station is idle, it waits for a period of time called DIFS - distributed interframe space
then it send a control frame - RTS - request to send.

2. After receiving RTS it waits for a period of time called SIFS - short interframe space.
then destination sends control frame called CTS - clear to send to source station - indication that destination is ready to receive.

3. source station sends data, after waiting for time equal to SIFS

4. Destination after waiting for a time equal to SIFS sends acknowledgement to show that frame is received. - needed cause source has no means to check for successful data arrival.

→ To inform other stations that a station is currently in access - collision avoidance.
- when RTS is sent it include time duration to occupy channel.
stations involved in transmission create timer called NAV - network allocation vector - time after which stations can check for idleness.

→ Each time a station sends an RTS, other stations start their NAV timer.

__/__/____

→ collision during when RTS is in transition.
Handshaking Period.
two or more stations may send RTS frame at the same time causing collision.

- there is no mechanism for collision detection.
- collision is assumed by sender if CTS is not received, back off mechanism is employed. sender tries again.

PCF

- implemented in infrastructure network [with AP]
- implemented on top of DCF for time sensitive transmission.
- PCF has contention free polling access method. AP performs polling for stations. - stations are polled sending any data they have to AP.
- PCF needs more priority over DCF
  - interframe spaces have been defined
  → SIFS
  → PIFS < DIFS

if at same time station wants to use DCF
AP wants to use PCF, AP has priority.
but due to this DCF may never gain access - to prevent this repetition interval is designed, whichever is repeated continuously it starts with a beacon frame.
when stations see a beacon frame NAV is set.
during repetion PCF can send and receive data, send and receive ACK using piggybacking.
after DCF has finished, PCF send a contention free end frame.

FRAGMENTATION

- wireless environment is very noisy ∴ corrupt frames have to be retransmitted.

It is easier to send smaller frames again than large ones

MAC layer has 9 fields.

2	2	6	6	6	2	6	0-2312	4
FC	D	AM 1	AM 2	AM 3	SC	AM 4	Frame Body	FCS

1. Frame control : defines type of frame
2. D : defines transmission duration & frame ID
3. 4 address fields
4. Sequence control : defines sequence number of frames.
5. Frame Body : contains information
6. FCS : contains CRC-32 error detection sequence.

TYPES OF FRAMES [IEEE 802.11]

1. Management Frames - initial communication b/w station & access points.
2. Control Frames - used for accessing channel & acknowledging :- RTS - 1011
   CTS - 1100
   ACK - 1101
3. Data Frames - used for carring data.

ADDRESSING MECHANISMS

→ 4 cases defined by values of FC field.

→ To DS and From DS

→ values can be either zero or 1 giving 4 - cases.

To DS	From DS	next device 1	previous device 2	final 3	original source 4
0	0	destination	source	BSS ID	N/A
0	1	destination	sending AP	source	N/A
1	0	receiving AP	source	destination	N/A
1	1	receiving AP	sending AP	destination	source

Case 1 : 00

not going to a distribution system - To DS
not coming from a distribution system - From DS
frame moving from one station in BSS to another

case 2 : 01

frame is coming from a distribution system
i.e an AP and going to a station.

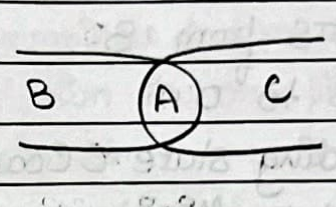
case 3 : 10

frame is coming from a station and going to
a distribution system AP.

case 4 : 11

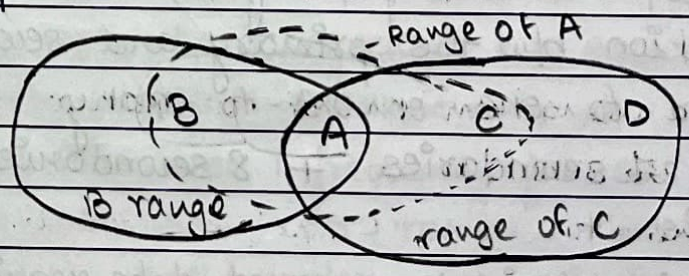
frame is going from one AP to another AP
wireless distribution
4 address to define original sender, destination
and intermediate AP

Hidden Station Problem.



- → B is located outside transmission range of C
- → C is located outside transmission range of B
- → A can hear any signal transmitted by B & C.
- → assume B is sending data to A and at the same time C is sending data to A
- → B and C cannot reach each other and ∴ thinks medium is free.
- → this results in collision at A and say, the stations B & C are hidden w.r.t A
- → solution - Handshake frames
- → RTS from B reaches A but not C
- → CTS from A reaches both B and C, hence C knows about hidden station and refrains transmission.

Exposed Station Problem.



- A is transmitting data to B
- C has data to send to D - it can be sent without interference with A to B.
- C is exposed to transmission from A and refrains sending. C - conservative & wastes capacity.

Handshaking will not help.
C cannot get CTS from B.
C can send RTS to D.
If A is in sending state C cannot hear CTS from D due to collision.

BLUETOOTH

- Wireless LAN technology
- it is an ad hoc network, network is formed spontaneously, devices find each other and make a network called a piconet.
- IEEE 802.15 defines a personal-area network (PAN)

ARCHITECTURE:

- defines 2 types of networks

1. PICONET

- also called a small net.
- can have upto 8 stations.
- one of them is a primary device and the rest are secondary.
- secondary stations synchronize their clocks and hopping sequence with primary stations.
- communication b/w the primary and secondary can be one-to-one or one-to-many.
- have max 7 secondaries + 8 secondaries are in parked state.
- activation of a device from parked state requires that a device goes into parked state.

__/__/____

2. SCATTERNET

- Piconets are combined to form a scatternet.
- secondary station in one piconet can be a primary in another piconet.
- It can receive and deliver messages - i.e a station can be a member of 2 piconets.

LAYERS IN BLUETOOTH

Applications
Profile
Data
L2CA player
Baseband layer
Radio layer

RADIO LAYER :

- equivalent to physical layer.
- low power devices
- 10 m range
- uses FHSS - frequency hopping spread spectrum to avoid interference from other devices.
- hops 1600 times per second i.e each device changes its frequency 1600 times per second.
- a devices uses 1 frequency for 625 μs - dwell time.
- Bluetooth uses TDD - TDMA - time division duplex TDMA - half duplex communication - both primary & secondary can receive & send but not at the same time.

single secondary communication. - if piconet has only 1 secondary device. Primary uses even slots and secondary

uses odd-numbered slots

eg: slot 0 - primary sends, secondary receives
slot 1 - primary receives, secondary sends.

Multiple secondary communication - more than 1 secondary is present.

primary uses even-numbered slot, secondary uses next odd numbered slot

eg:

slot 0 - $P \longrightarrow S_1$

slot 1 - $S_1 \longrightarrow P$ as previous frame was addressed to $S_1 P$

slot 2 - $P \longrightarrow S_2$

slot 3 - $S_2 \longrightarrow P$

Physical Links.

1. SEQ - Sychronous connection oriented link
- avoiding latency is more important than integrity.
- physical link is created b/w primary and secondary
- Basic unit of connection b/w 2 slots - one for each direction.
- damaged packets are not retransmitted.
- real time audio transmission
- secondary can create upto 3 SEQ links with primary.

2. ACL - asychronous connectionless link
- is used when data integrity is more important than avoiding latency.
- if payload is damaged it is retransmitted.
- can use any number of slots to achieve max data rate.

FRAME FORMAT.

72 bits	54 bit						
Access code	Header	Data					
	Address	Type	F	A	S	HEC	

1. Access code : 72 - bits - sychronization bits and identifier of primary
2. Header : 54 bit - repeated 18 bit pattern.
   1. Address - 3 bit, define upto 7 secondaries. if its zero, its for broadcast communication.
   2. Type - 4 bit - defines type of data
   3. F - 1 bit - flow control
   4. A - 1 bit - for acknowledgement - uses Stop and wait ARQ
   5. S - 1bit - sequence number
   6. HEC - 8 bit - header error correction is a checksum.

→ If 3 identical 18 - bit sections are same the bits are accepted.

3. Payload : 0 - 2740 bits, main data.

L2CAP

→ logical link control and Adaptation protocol.

→ data exchange on an ACL link.

- Multiplexing - accepts data from upper layers, frames them and sends to baseband layer.
- Segmentation & reassembly - divide large packets into segments and adds extra info to fill gap. segments at source and reassembles at destination
- QOS - quality of service - best effort service
- Group management.

__/__/____

CONNECTING DEVICES.

→ are used to connect LAN's or segments of LAN's

5 categories of connecting devices.

1. Those which operate below physical layer - passive hub
2. Those which operate at the physical layer - repeater or active hub
3. Those which operate at the physical & data link layer - bridge or two-layer switch.
4. Those which operate at physical, data link & network layers - router or 3-layered switch
5. Those which can operate at all 5 layers - gateway.

PASSIVE HUBS

→ connects wires coming from different branches.

→ In star-topology - passive hub is a point where signals coming from different stations collide hub is the collision point

→ Its located below the physical layer.

REPEATERS

→ only at the physical layer.

→ signals that carry information can travel a fixed distance before attenuation endangers it.

→ a receptor receives a signal and before its too weak or corrupted and regenerates original bit pattern.

→ repeater does not actually connect two LAN but connects two segments of same LAN

→ length of cable is restricted to 500m, to extend it, cable is divided into segments and repeaters are added which is called a

segment.

→ amplifier amplifies everything equally - even noise

→ Repeater must be placed at such a place that signal reaches it before noise.

ACTIVE HUBS

→ multiport repeater

→ create connections b/w stations in a physical star topology.

BRIDGES

- function : operates in both physical & data link layer.
- regenerates signal it receives.
- physical layer : regenerates incoming signal
- data - link layer : examine MAC address.

→ Bridge has filtering capabality. It analysis the destination address of a frame and decide whether to forward it or drop it.

→ Maintain a table that helps in filtering. Table maps MAC address to ports. The frame that comes has an address, the bridge consults the address table and takes action

TRANSPARENT BRIDGE

→ connected stations are completely unaware of the bridge's presence.

→ + and - bridges does not require station reconfiguration

TB must meet 3 criteria

1. Frames must be forwarded from 1 station to another.
2. Forwarding table is automatically created by learning frame movements.
3. system loops must be prevented.

Learning Process :

- A → D. Bridge has no entries of either A or D frame is sent out through all ports (flooding) By the source address and learns that A is on port 1
- when E → A, Bridge forward frame only to port 1. source address of E is added
- learning process continues
- destination address : forwarding decisions.
  source address : for adding entries.
- TB should also implement mechanisms to prevent network loops leading to broadcast storms.

LOOP PROBLEMS

- admins have redundant bridges, if incase a bridge fails, which creates loops

→ A → D, both bridges forward the frame and update their tables.

→ two copies of frame are now on LAN 2.
Each bridge forwards the copy but neither have information on destination D.
Both bridges flood frame onto another LAN.
and process repeats.

→ loop forwarding & flooding continues.
Each iteration gives fresh copies of frames.

__/__/__

SPANNING TREE

- graph which there is no loop.
- creating a topology in which LAN can be reached from any other LAN through a single path.
- physical topology cant be changed but logical topology can be established.
- To find spanning tree - each arc (connection b/w LAN & bridge) is assigned a cost - min hops, min delay, max bandwidth.

1. Identify bridge with smallest ID as root bridge.
2. Find shortest path from root bridge to every other bridge.
3. combine shortest path
4. mark ports on spanning tree, forwarding & blocking ports.

Since there is only one path from any other LAN to any LAN, uniqueness ensures loops are prevented.

→ each bridge has a software pack that carries out process dynamically, they send messages called Bridge protocol data units to update spanning tree.

BPDU inform changes - bridge failure, additions & deletions

SOURCE ROUTING BRIDGES

- method for prevention of loops with redundant bridges.
- filtering, forwarding & blocking are done by stations

at the source.

→ sending station determines bridge route

→ Frame not only includes source & destination but also all bridges to be visited.

→ source gets bridge addresses through exchange of special frames to destination before sending data frame.

BRIDGES CONNECTING DIFFERENT LANS.

→ Bridges that connect different LANS have challenges due to protocol differences.

1. Frame Format :
2. Max data size : incoming frame might be too large for destination LAN. [segment & reassemble]
3. Data Rate : LANS have different data rate that cause buffering.
4. Bit Order : Bit sending order varies. [most & least significant]
5. Security : encryption
6. Multimedia support:

TWO- LAYER SWITCH

- like to bridge with multiple ports
- faster performance - switching factor.
- large port capacity for individual stations. [unique]
- eliminate collision.
- filters based on MAC address.

ROUTER {like to 3 layer switches}

→ routes packets based on logical addresses.

→ connects LANs to WANS - has a routing table.

→ routing tables are dynamic.

__/__/____

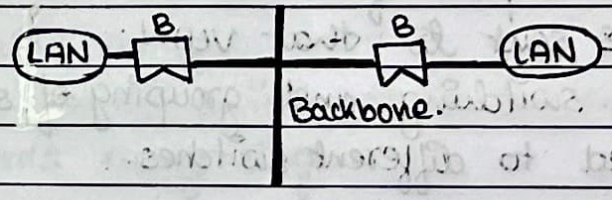
GATEWAY

- operates on all 5 layers of the internet
- it takes an application message reads it and interprets it
- can be used as a connecting device between two devices using different models.
- provide security
- ~~gi~~ filter unwanted messages from application layer.

BACKBONE NETWORKS

1. BUS BACKBONE

- bus backbones are normally used as backbones to connect different stations, they can either comprise of a LAN or another backbone.



→ if LAN sends frame to another device in same LAN, bridge blocks frame, from entering backbone

→ if station has to send it to a station in another LAN, bridge passes frame to backbone.

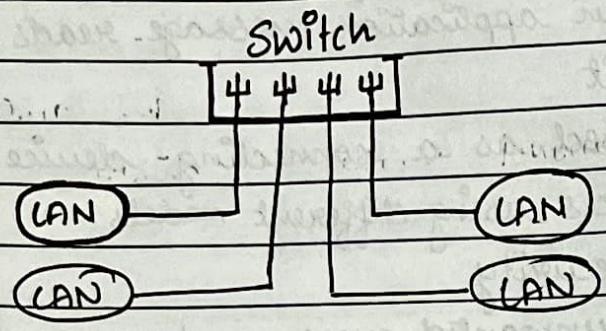
→ bridge connected to backbone has table showing all stations on the side of LAN.

→ blocking & delivery is based on this table

2. STAR BACKBONE

- collapsed or switched backbone.
- backbone is a star / just one switch.
- used as distribution backbones
- LAN serves each particular floor.

- backbone connects these LANS.



VIRTUAL LANS.

- LAN configured by software, not by physical wiring.
- moving or switching a station from one LAN to another gets easier
- since a station is part of a LAN through software
- all stations part of a VLAN can receive broadcast messages sent to that VLAN.
- allows switching and grouping of stations connected to different switches.

MEMBERSHIP.

- Port numbers: admin can define stations connecting to ports 1, 2, 3 and 7 belong to VLAN1 and the rest to VLAN 2.

- MAC address
- IP Address.
- Multicast IP address

Configuration : 3 ways.

1. Manual configuration : manually types in the software.
2. Automatic : criteria defined by administrator, define project number as criterion, when user changes project, they migrate to a new VLAN.
3. Semiautomatic :
   initialize manually
   migration automatically.

COMMUNICATION B/W SWITCHES.

- each switch needs to know not only which station it belongs to but also which VLAN and membership status of stations of other switches.

Table Maintenance

- broadcast frame - switch creates an entry in table and records everything.

Frame tagging.

- when frame travels b/w switches, extra header is added to MAC frame to define destination.

TDM

Trunk b/w switches is divided into time shared channels.

VLAN 1 ⟶ channel 1

receiving switches determine the channel from which it arrived.

Advantages.

→ Cost & time reduction.
migration cost
hardware cost
easier & quicker to connect / move by software.

→ create virtual work groups.

→ security : people in same group can broadcast msgs with guaranteed assurance that users in other groups will not receive it.