WIRELESS LAN's (LOCAL AREA NETWORK) -

- WLAN is a network that allows devices to connect & communicate wirelessly within an area using radio waves ; instead of wired connection
- Eliminates need for physical cables.
- Uses CSMA/CA (Carrier Sense Multiple Access with Collision Detection)
- IEEE 802.11 (WiFi) defines the communication rules for WLAN.

Network Architecture -

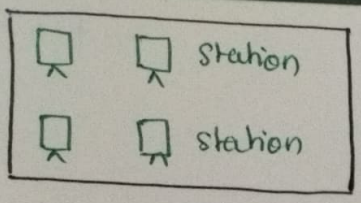
IEEE 802.11 defines 2 types of services :

1) Basic Service Set (BSS) — Basic building block of WLAN. It consist of wireless stations (STA) that communicate with each other at physical layer. There are 2 types of BSS :-

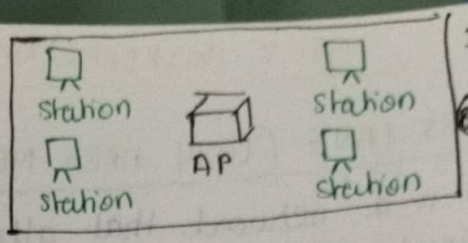
i) Independent BSS (Ad-Hoc Network) :
→ Does not use AP (Access Point) to manage communication.
→ Each device acts as transmitter and receiver both, forming a temporary network. (peer-to-peer manner).
→ Used in short range communication.
→ Eg. File sharing between laptops.

ii) Infrastructure BSS :
→ Include AP that acts as central hub for communication.
→ Wireless stations communicate with each other via AP.
→ Used in homes, offices, universities & public places (Hotspots).
→ Can connect to wired network or other BSS's
→ Eg. A Home WiFi router acts as AP, connecting all devices to internet.

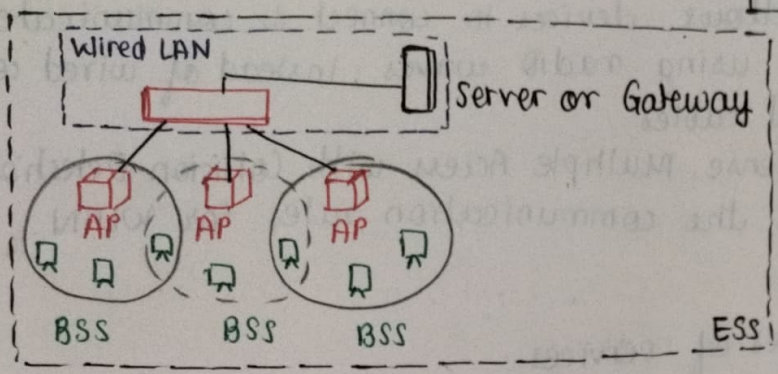
2) Extended Service Set (ESS) — Consist of two or more BSS's with Access Points (APs). It connects multiple BSS's using Distributed System (DS). It is used to expand network coverage & enable roaming between access points.
- IEEE 802.11 does not specify the type of DS ; it can be Ethernet or any IEEE LAN.
- ESS contains 2 types of stations :
i) Mobile stations - regular devices inside BSS like laptops, phones, etc.
ii) Stationary stations - APs that connect to wired LAN.
APs talk to each other through a wired connection helping devices to stay connected.
ESS creates big wifi network, so roaming is possible.



Ad-hoc network
(BSS without AP)



Infrastructure (BSS with AP)



When BSSs are connected, the stations within reach of one another can communicate without AP. But communication betn 2 stations in 2 different BSS's occurs via 2 AP's.

Components in IEEE 802.11 network / WLAN –

1) **Stations (STA)** – Devices connected to WLAN (like laptops, smatphones, etc) Each station includes a wireless network interface controller (NIC) for communication.
2) **Wireless Access Point (WAP)** – Acts as a central hub in infrastructure mode. Connects wireless stations to wired network or other wireless devices.
3) **BSS** – Fundamental building block of WLAN. 2 types
   Infrastructure BSS → Stations communicate via an AP.
   Independent BSS → Stations communicate directly without an AP.
4) **ESS** – Combines multiple BSS using DS. Provides extended coverage & seamless roaming APs.
5) **DS** – Connects APs in an ESS, typically using a wired LAN like Ethernet.

These components work together to enable flexible & scalable wireless communication in IEEE 802.11 networks.

IEEE 802.11 Station Types: No Transition, BSS Transition, ESS Transition.

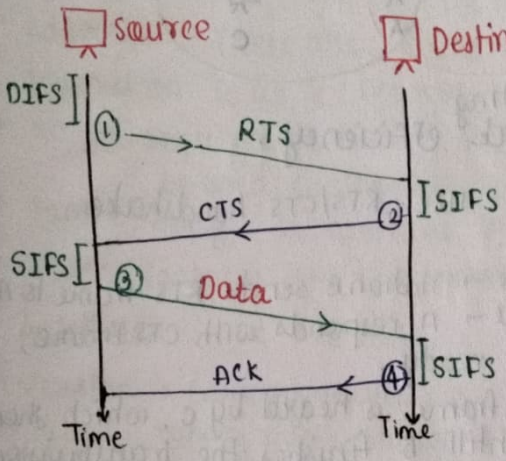
Physical Layer –

Mode	Technology Used	Speed	Frequency	Remarks
802.11 IR	Infrared	1-2 mbps	Infrared	Uses lightwaves instead of radio signals, rarely used.
802.11 FHSS	Frequency Hopping Spread Spectrum	1-2 mbps	2.4 GHz	Hops betn different frequencies to reduce interference.
802.11 DSSS	Direct Sequence Spread Spectrum	1-2 mbps	2.4 GHz	Spreads signal across a wider bandwidth
802.11a OFDM	Orthogonal frequency Division Multiplexing	54 mbps	5 GHz	High speed transmission but limited range.
802.11b HR-DSSS	High-Rate DSSS	11 mbps	2.4 GHz	First widely used wifi standard, good range but slow
802.11g OFDM	OFDM + Backward compatible with 802.11b	54 mbps	2.4 GHz	Combines speed of 802.11a with range of 802.11b

MAC Sublayer – It manages access to the wireless medium & ensures reliable data transmission between devices in WLAN.
Medium Access Control (MAC) coveres 3 functional aves :–
① Reliable data delivery ② Access control ③ security.
IEEE 802.11 standards has 2 MAC techniques – 1) DCF & 2) PCF

DISTRIBUTED COORDINATION FUNCTION (DCF) :–

It allows devices to share the wireless channel without a central controller by using carrier sense Multiple Access with Collision Avoidance (CSMA/



1 → The sender sends RTS (Request to Send) to the receiver.
2 → The receiver responds with a CTS (Clear to Send), indicating its ready.
3 → The sender transmits the data frame.
4 → The receiver sends ACK to confirm successful reception.

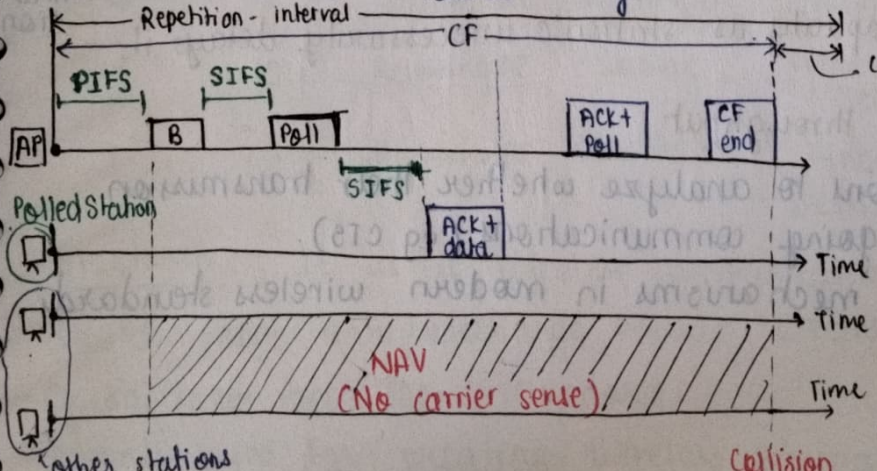
RTS/CTS helps to avoid collisions.
SIFS → short interframe space
DIFS → distributed interFrame space

* Before sending frame, the source station senses the channel.
IF idle, DIFS → RTS
IF busy, backoff → keep checking until idle.

NAV (Network Allocation Vector) – virtual carrier sensing mechanism used to avoid collisions in wireless communication.

POINT COORDINATION FUNCTION (PCF) :–

Uses a centralized method to control acces to the wireless medium. The Access Point (AP) decides which device gets to send data, ensuring fewer collisions & lower delays.



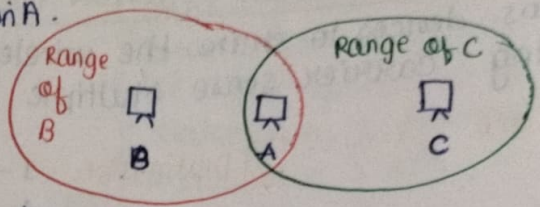
PIFS → PCF inter-frame Spacing

	Control Type	Access Method	Best for	Collision Handling	Delay	Priority	Network Requirement
DCF	Decentralized	CSMA/CA	Web browsing file transfers	Use backof mechanism	High	low	works in Ad-hoc & infrastructure mode.
PCF	centralized	Polling	Voice, VC, streaming	No collision	low	High	Requires an AP

Hidden and Exposed station problem -

Hidden station problem : When 2 devices (B & C) are out of each others transmission range but both want to communicate with a common device (A). Since B & C cannot detect each others transmissions, they may send data simultaneously to A, causing collision at A.

Eg · • Station B is transmitting data to station A.
• Station C, which is out of range of B, also wants to send data to A.
• Since C cannot hear B's transmission, it assumes the channel is free & starts transmitting.
• This leads to collision at A, reducing network efficiency.

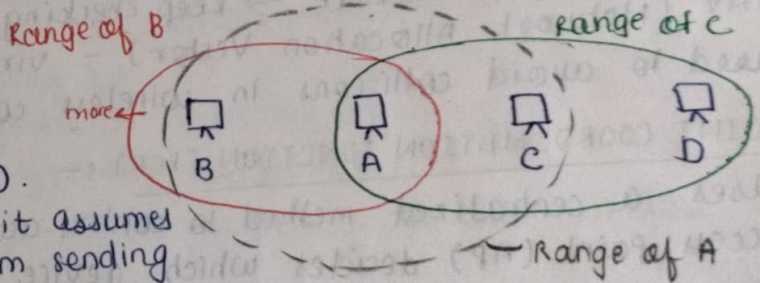


Effects - i) Collisions = lost data packets
ii) Network throughput decreases due to retransmissions.
iii) wastes bandwidth & increase latency.

Solution - use RTS/CTS handshake mechanism.
• RTS frame → Station B sends RTS frame to A
• CTS frame → A responds with CTS frame, that its ready.
• The CTS frame is heard by C, which then waits untill B finishes the transmission

Exposed station problem:

When a station unecessarily refrains from transmitting because it detects a nearby ~~transition~~ transmission that would not actually cause interference.



Eg. • Station A is transmitting data to B
• Station C, which is in range of A but not B, wants to send data to D.
• Since C hears A's transmission, it assumes the channel is busy & refrains from sending data, even though its transmission would not interfere with A-B communication.

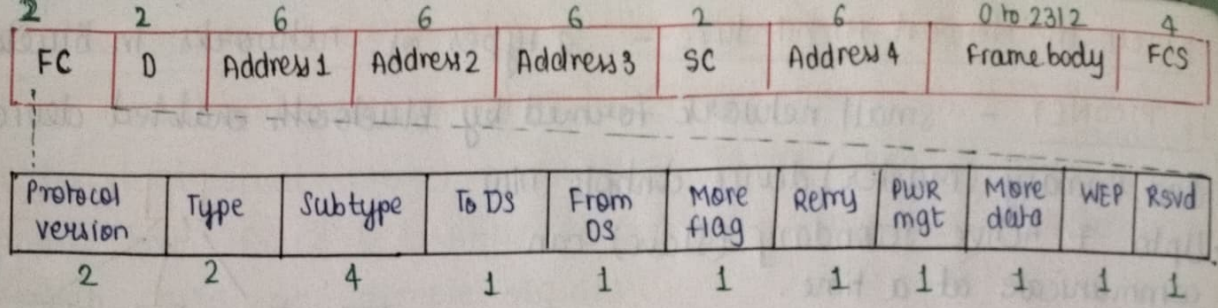
Effects - i) wastes network capacity as station C unecessarily delays its transmission.
ii) Reduces overall network throughput.

Solution - i) Allowing stations to analyze whether their transmission would interfere with ongoing communications (eg CTS).
ii) Advanced scheduling mechanisms in modern wireless standards like WiFi 6 (802.11ax)

MAC Frame Format -

MAC layer frame consist of 9 fields

Frame control
Duration
Addresses
Sequence control
frame body
Frame Check Sequence



- FC → Frame Control : Defines types of frames & some control info.
- D → Duration : This defines the duration of transmission that is used to set the value of NAV. This frame defines frame ID.
- Addresses : There are 4 addresses each 6 bytes long. The meaning of each address depends on To DS & From DS subfields.
- SC → Sequence control : This defines the sequence number of the frame to be used in the flow control.
- Frame Body : It contains info based on type and subtype defined in FC field.
- FCS : Contains CRC-32 error detection sequence.

Subfields in FC field :—

1) Version → Current version is 0
2) Type → type of info : management (00), control (01) or data (10)
3) Subtype → subtype of each type
4) To DS → } Defined later
5) From DS → } Address interpret
6) More Flag → when 1, means more fragments
7) Retry → when 1, means retransmitted frame
8) Pwr mgt → when 1, mean station is in power management mode.
9) More data → when 1, means station has more data to send.
10) WEP → wired equivalent privacy.
11) Rsvd → Reserved

Addressing Mechanism —

To DS	From DS	Address 1 (Receiver)	Address 2 (Transmitter)	Address 3 (BSS ID)	Address 4 (Original Source)
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Original Source	N/A
1	0	Receiving AP	Source	final Destination	N/A
1	1	Receiving AP	Sending AP	Final Destination	original Source

Bluetooth — It is a wireless communication technology designed for short-range data exchange between electronic devices.

- Operates on IEEE 802.15 standard.
- Mainly used for creating Wireless Personal Area Networks (WPANs).

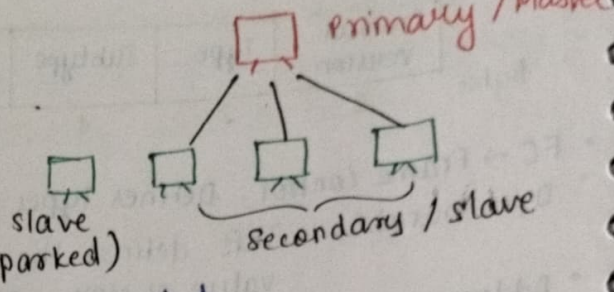
Key features : i) Ad-hoc networking
ii) Short-range communication
iii) low power consumption.
iv) Supports voice & data communication.
v) operates in 2.4 GHz ISM band

Bluetooth Network Architecture – 2 types of networks in Bluetooth

1. PICONET – Small network formed by Bluetooth enabled devices.

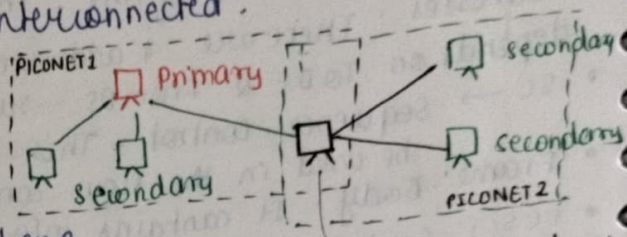
- One Primary (Master) device controls n/w.
- Upto 7 Active Secondary (Slave) can communicate at a time.
- Additional devices can be in a parked state.

Eg. Bluetooth headset connecting to phone.



2. SCATTERNET – multiple Piconets are interconnected.

- A single device can act as secondary in one piconet & primary in another.
- Allow communication betⁿ multiple n/w



Eg. Laptop connected to wireless mouse & phone
Piconet 1 Piconet 2.

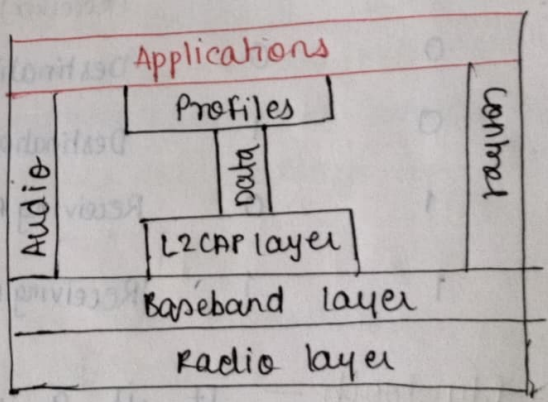
Bluetooth Architecture layers –

1) Physical layer (Radio layer) – Defines range and power levels.
- Uses 2.4 GHz ISM band with frequency hoping to avoid interference.

2) Baseband layer (Link layer + MAC) – Handles device discovery, synchronization and data transfer.

3) L2CAP (Logical Link Control & Adaption Protocol) – Splits & reassembles large data packets.

4) Application & Profile layer – Defines Bluetooth services.



Operational State –

Standby → Devices is inactive but listening.
Inquiry → Devices search for Bluetooth connection
Page → Device establishes a connection.
Connected → Active communication mode.
Sniff → low power mode with periodic wakeup.

Disadvantages of Bluetooth –

1) Short range (~10m)
2) Slow speed (~3 mbps)
3) Inference (wifi, microwaves)
4) Security risks (hacking threats)
5) Limited connections (upto 7)
6) Battery drain (on mobile devices)
7) Compatibility issues (older devices)
8) High latency (not ideal for real time use)

WiMAX (Worldwide Interoperability for Microwave Access) –

- Wireless broadband communication technology based on IEEE 802.16 standard.
- Provides high speed internet access over large areas & servers
- Supports both fixed & mobile connectivity, making it suitable for urban, rural and remote regions.

Advantages → • Wide coverage area.
• High-speed Internet
• Cost-Effective Deployment
• Flexible → supports both fixed & mobile applications.
• Alternative to wired Broadband
• Support for Multiple Appln.
• Interoperability
• No need for cables.

Comparision between:

Parameter	Bluetooth (IEEE 802.15)	WiFi (IEEE 802.11)	WiMAX (IEEE 802.16)
1) Protocol	802.15	802.11	802.16
2) Purpose	Short range device communication (PAN)	Wireless local area networking (WLAN)	Wireless broadband internet (MAN/WAN)
3) Range	10m - 100m	30m - 300m	Upto 50km
4) Speed	Upto 3 Mbps	Upto 9.6 Gbps	Upto 70 Mbps
5) Topology	Piconet, scatternet	Infrastructure or Ad-hoc	Point-to-Multipoint
6) Mobility	Low	Moderate	High
7) Performance	Moderate	High	High
8) Modulation	FHSS	OFDM, DSSS	QPSK
9) Main use	Wireless peripherals (headphones, keyboards).	Home, office & Public wifi networks.	Broadband internet in rural & urban areas.
10) Security	AES encryption, Secure paring	WPA2, WPA3 encryption	Strong encryption (AES, EAP)
11) Power consumption	Low	Medium	High

	Defn	Speed	Mobility	Cost	Security	Eg.
Wired Transmission	uses physical cables for data transfer	fast	Limited	expensive	More	Ethernet, fibre optics, landline phones.
Wireless Transmission	uses radio waves, IR or satellite for data transfer.	slow	High	Cheap	Less	Wi-Fi, Bluetooth, 4G/5G, satellite communication.

Characteristics of WLAN

1. Attenuation - weakening of signal strength as it travel through obstacles ie more distance = weak signal.
2. Inference - disrupts of wifi performace due to other signals
3. Multipath Propogation - wifi signals bounces off surfaces and reach the receiver at different times, causing disortion
4. Errors - Data packets can get lost or corrupted

Design Goals of WLAN

1. Operational Simplicity - simple to setup & simple to connect.
2. Saves Battery - uses less power so laptops & phones last longer.
3. Low cost - Works in free frequency bands.
4. Handles Interference - Should work smoothly even with other wireless signals around.
5. Works everywhere - must follow rules of different countries so it can be used worldwide.
6. Secure - should protect data from hackers.
7. Safe to use - No harm to health & no inference with medical devices
8. Good Quality - Support VC, gaming & streaming without lag
9. Works with other network - Can connect with wired n/w & internet without any issues.