(a). IEEE 802.11

→ Popularly known as wifi (Wireless LAN).

→ WLAN uses high frequency radio waves instead of cables for connecting the devices in LAN.

→ Users connected by WLANs can move around within the area of network coverage.

→ Architecture: The main components include:

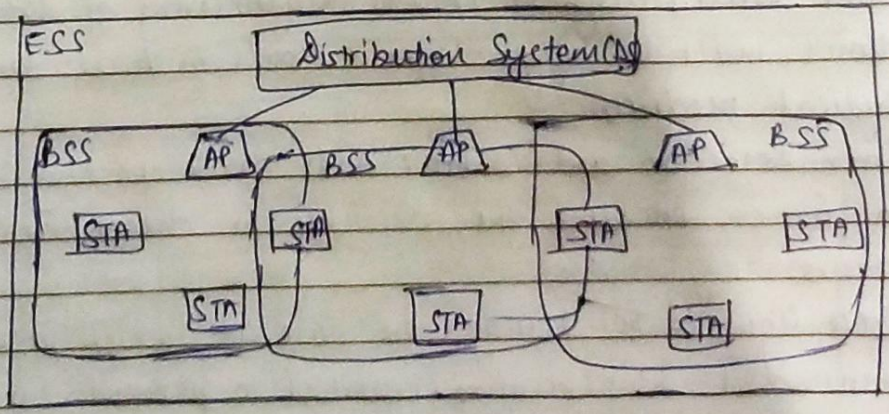
(a). Stations (STA): All the devices and equipments connected to WLAN. It can be: (1) WAP (Wireless Access Point): Wireless routers
(2). Clients: Workstations, computers, laptops, printers, etc.

(b). Access Point (AP): Central device that connects STAs to wired N/w. Acts as a bridge b/w wireless & wired n/ws allowing wireless n/w to access resources of wired N/w.

(c). Basic Service Set (BSS): Group of STAs communicating at Physical layer level. 2 Types:
(1). Infrastructure BSS: devices communicate with other devices through Access Points (APs)
(2). Independent BSS: devices communicate in adhoc manner.

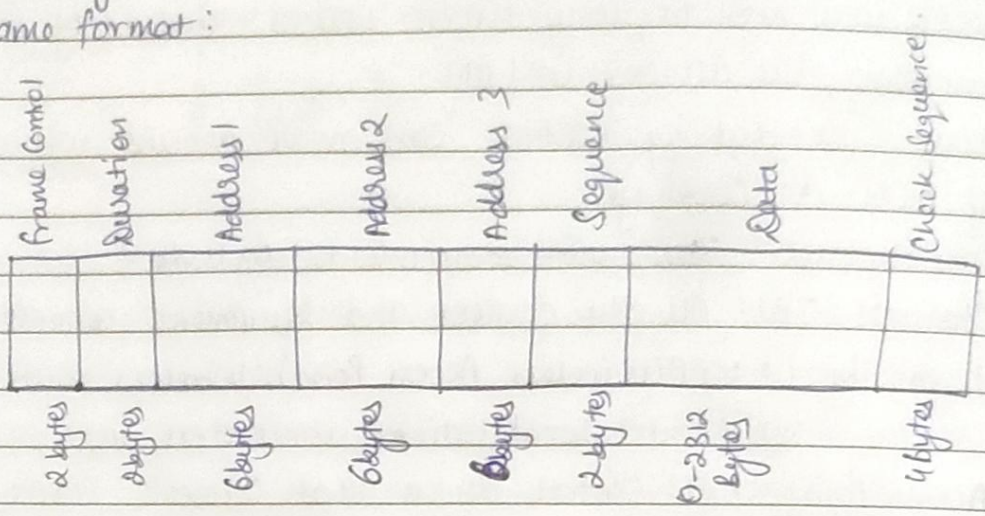
(d). Extended Service Set: Collection of interconnected BSSs. Allows users to roam b/w different BSSs within same ESS.

(e). Distribution System (DS): Responsible for interconnecting multiple BSSs and allows exchange of data b/w them.



→ Provides authentication, security.
→ Includes various ~~security mechanisms~~ frequency bands, including 2.4 GHz & 5 GHz bands.

(*) Frame format:



(*) Protocol Architecture:
Organized into several layers similar to OSI Model:

① Physical layer (PHY): → deals with physical aspects of wireless com
→ Defines modulation techniques, frequency bands, data rates & other hardware related parameters.

② Logical Link Control (LLC): sits b/w the MAC layer & upper layers
→ Responsible for link management and encapsulation.
→ Primary functions include:

(a) Frame addressing and identification: LLC assigns a unique address to each frame that allows devices to identify and process the frames that are intended for them.

(b) Frame Multiplexing: It enables multiplexing of data.
→ Allows multiple higher-layer protocols to share same physical medium.

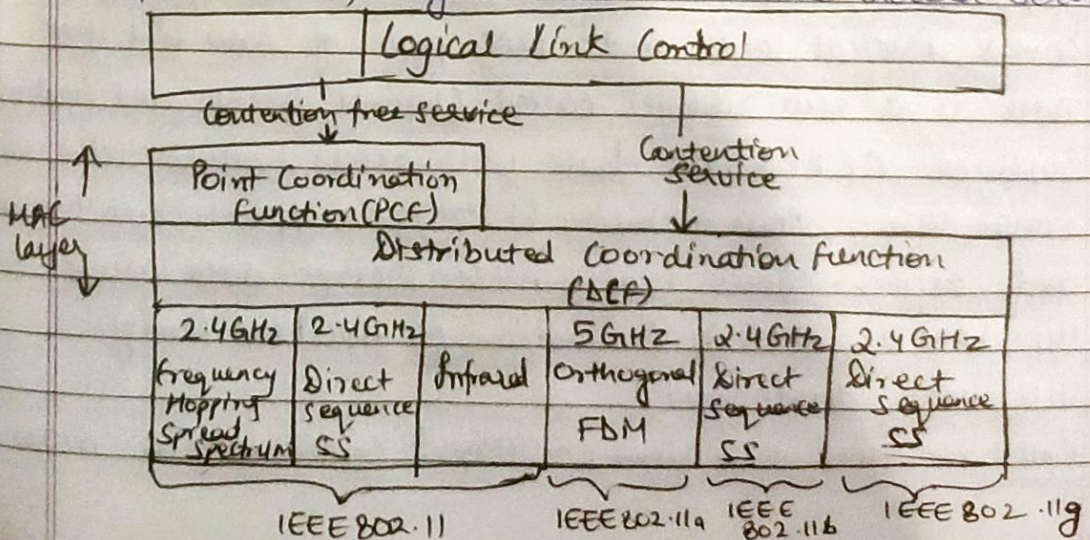
(c) Error Detection and Control: Adds error checking information to frames, enabling the receiver to detect and correct errors.

(d) Flow Control: Manages the rate at which packets are transmitted b/w devices. Essential to prevent n/w congestion.

(c) Frame Control and Management: Handles various control frames, such as frame acknowledgement & frame retransmission.
→ Important for maintaining reliability.

(d) Frame format and Encapsulation: defines the format in which data packets are encapsulated.
Specifies how data is packaged into frames and how headers, trailers and data payloads are structured.

(3) Medium Access Control:
→ Manages access to shared wireless medium.
→ Includes functions like frame management, error checking, fragmentation.
→ Serves as a bridge b/w higher layer protocols & physical layer.
→ Ensures that data is transmitted efficiently & reliably in a shared wireless environment.
→ Offers support for roaming, authentications & power conservation.
→ Basic services provided include mandatory asynchronous data service and optional time-bounded service.
→ Distributed coordination function (DCF): uses CSMA/CA access method as WLAN can't implement CSMA/CD. It only offers asynchronous service.
→ Point Coordination function (PCF): Implemented on top of DCF. Mostly used for time-service transmission.
It offers both, asynchronous and time bound service.



(*) HIPERLAN:

→ High Performance Local Area Network (HIPERLAN).
→ wireless standard derived from traditional LAN environment.
→ Can support multimedia and asynchronous data effectively at high data rates of 23.5 Mbps.
→ Does not necessarily require any access point for its operation.
→ Radio waves are used instead of cables as a transmission medium to connect stations.
→ Either the radio transceiver is mounted on movable station and no base station has to be installed seperately, or a base station is needed in addition per room.
→ Stations may be moved during operation pauses.
→ Max data rate depends upon distance b/w the stations.
→ Short distance & asynchronous transmission, data rate → 20 Mbps.
→ upto 800 m distance, data rate → 1 Mbps, others → 64 Kbps (at least)
→ Main idea is to provide an infrastructure & adhoc wireless with low mobility and a small radius.
→ Supports isochronous traffic with low latency.
→ HiperLAN family has 4 different versions.
→ Key feature is the integration of time-sensitive data transfer services.
→ Family: Hiperlan 1, Hiperlan 2, HiperAccess & Hipereink.

(*) HiperLAN 1: → Goal was higher data rate than 802.11.
→ Covers Physical layer and MAC part of Data link layer.
→ There is a new sublayer called Channel Access and Control Sublayer (CCAC$). It deals with access requests to the channels.
→ range 50 m, slow mobility (1.4 m/s), supports synchronous and asynchronous traffic, video 2 Mbps, data 10 Mbps.

(*) HiperLAN 2: → Next Generation of HiperLAN family.
→ Still under development.
→ Goal - Providing high speed (≈54 Mbps) communication access.

→ connection-oriented, secure, flexible, etc.

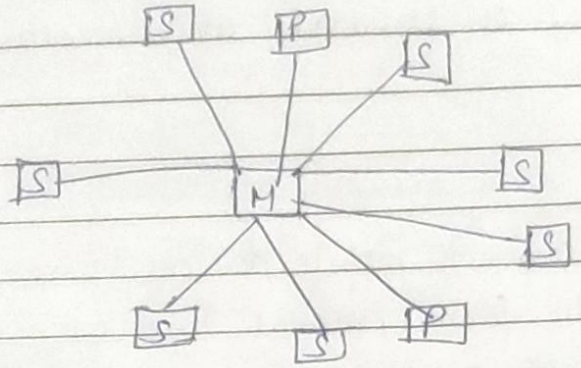
(*) Hiperaccess & Hiper Link: parallel to developing Hiperlan2, work is being done on standards complementary to HIPERLAN 2.

(*) Bluetooth:

→ Technology that connects mobile devices wirelessly over a short range to form Personal Area Nlw (PAN).
→ Initially standardized as IEEE 802.15.1
→ A PAN can be created within a 10m radius.
→ Presently, 2 to 8 devices may be connected.
→ Allows devices within the range to find Bluetooth devices and connect with them. This is called pairing.
→ Once paired, the devices can transfer data securely.
→ low power consumption as low implementation cost than wifi.
→ Range and transmission speeds are lower than Wifi.
→ BT version 3.0 and Higher versions can deliver data rate of 24Mbps.
→ Two types of Bluetooth Nlws:
(a). Piconets (b). Scatternets.

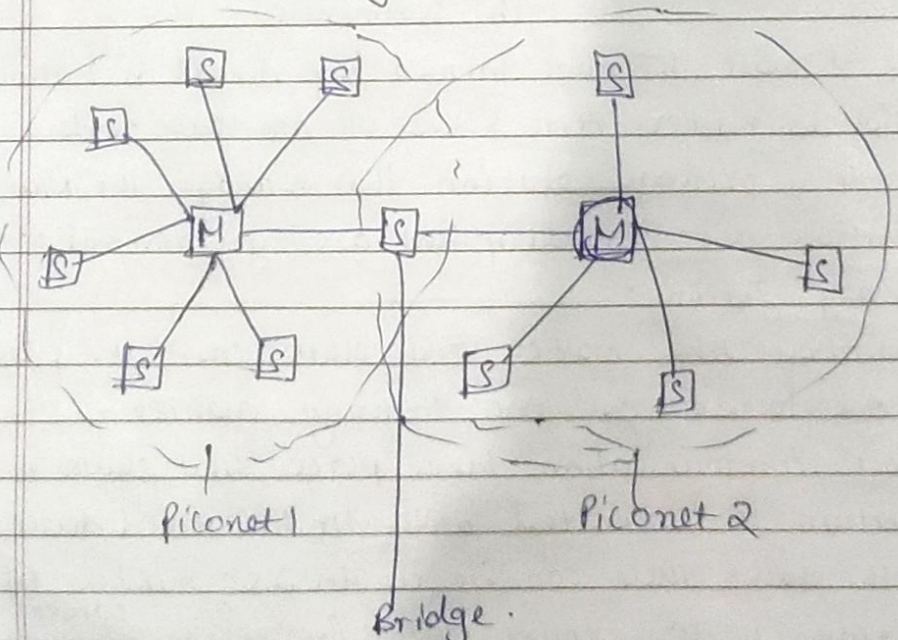
(*). Piconets: → Small BT nlws formed by atmost 8 stations.
→ One station is master node & rest 7 are slave nodes.
→ Master node is primary station that manages the Nlw.
→ Slave stations are secondary that are synchronized with the primary station.
→ Communication blw master and slave can take place in either one-to-one or one to many manner.
→ No direct communication takes place blw slaves.
→ Each station is associated with 48 bit fixed device address.
→ Besides the slaves, there can be up to 255 numbers of parked nodes in low power state for energy conservation.

→ The only work they do is respond to a beacon frame for activation from master node.



M - Master Node
S - Slave Node
P - Parked Node.

(*). Scatternets: → Interconnected collection of 2 or more piconets.
→ formed when a node in a piconet acts as a slave in another piconet. (Node can be master as well as slave).
→ This node is called the bridge b/w two piconets.
→ Offers the advantage of expanding Bluetooth N/ws by enabling more devices to communicate.
→ Allows for more flexible & scalable BT applications.
→ Managing can be challenging and requires careful design and protocol Management.



(v): IEEE 802.15

→ low cost, low data rate wireless access technology that is used for devices that operate or work on batteries.

→ Describes how low Rate wireless Personal Area Networks (LR-WPANs) functions.

→ focuses on developing standards for wireless PANs.

→ Typically designed for short range, low power wireless comm.

→ Key standards include:

(a). IEEE 802.15.1 (Bluetooth).

(b). IEEE 802.15.4 - Specifies Physical (PHY) and Medium Access Control (MAC) layers for low rate WPANs.
Designed for low complexity applications.

(c). IEEE 802.15.4a (UWB): Extends IEEE 802.15.4 by adding support for ultra WideBand (UWB) communication.
Allows for precise location & tracking applications.

(d). IEEE 802.15.4g: (Smart Utility N/ws) It defines Physical and MAC layer specifications for wireless communications.

(e) IEEE 802.15.4e: (Time-Synchronized Channel Hopping)
An ammendment to IEEE 802.15.4 standard. Improves reliability

(f). IEEE 802.15.5 (Mesh Networking): Defines architecture & protocols for wireless mesh networking in WPANS. Enhances N/w coverage.

(g). IEEE 802.15.6 (Body Area N/ws): used in medical & health care applications like wearable health monitoring devices.

(h). IEEE 802.15.7 (Visible Light Communication): Data is transmitted using visible light. Often used for indoor positioning and communication.

→ IEEE 802.15 standards cover a wide range of wireless communication technologies.

(*) Properties:

① Standardization and alliances: It includes:
   (a) zigbee
   (b) 6LOWPAN (IPV6 over low Power WPAN)
   (c) zigbee IP
   (d) wireless HART
   (e) Thread.

② Physical layer.

③ MAC layer

④ Topology

⑤ Security

⑥ Competitive technologies.

(*) Advantages:

① cheap cost
② long battery life
③ Quick installation
④ Simple
⑤ Extensible protocol stack

(*) Disadvantages:

① Causes Interference
② doesn't employ frequency hopping approach.
③ unbound latency
④ Interference susceptibility.

(*) Applications:

① Wireless Sensor N/ws
② Buildings & Home Automation
③ Remote controllers & interacting toys.
④ Automotive N/ws

(*) MANET CHARACTERISTICS ROUTING:

→ In mobile ad hoc N/W (MANET), nodes do not know the topology of their N/w.

→ Nodes need to discover the topology on their own as the topology in adhoc N/w is dynamic topology.

→ A new node on entering the n/w must announce its arrival and presence and should listen to similar announcements by other nodes.

MANET Routing Protocols

Proactive (DSDV, GSR) | Reactive (DSR, AODV) | Hybrid (ZRP)

① Proactive Routing Protocols:

→ Also known as table driven routing protocols.
→ Each mobile node maintains a seperate Routing table which contains info. of all possible destination nodes.
→ Routing tables are updated periodically.
→ doesn't work well for large n/ws.

(a) Destination Sequenced Distance Vector Routing (DSDV) Protocol:

→ Extends Distance Vector Routing Protocol.
→ Based on Bellman ford Routing Algorithm.
→ Not suited for mobile ad hoc n/w due to count to infinity problem. Solution is Destination Sequenced DVRP.
→ Destination sequence number is added with every entry.
→ A node includes new update only if the route is updated and mentioned with a higher sequence number.

(b) Global State Routing (GSR): Extends link state routing of wired n/w.

→ Based on Dijkstra's Routing Algorithm.
→ Link state routing was not suited for Adhoc n/w bec each node floods the info into the whole n/w, which leads to congestion.
→ Solution is Global State Routing Protocol.
→ It doesn't flood the link state routing packets globally into n/w.
→ Each ~~node maintains~~ Mobile node maintains one list & 3 tables namely adjascency list, topology table, next hop table & distance table.

→ 2 Phases < Route Discovery / Route Maintenance.

Date: Page:

(2) Reactive Routing Protocols: → On demand Routing Protocols.
→ The route is discovered only when it is required / needed.
→ Process of Route discovery occurs by flooding Route Request Packets throughout the mobile Nlw.
→ Source Node stores complete path info / Intermediate nodes need not maintain Routing Information.

(a) Dynamic Source Routing Protocol (DSR)
→ Source node stores complete path info. Intermediate nodes need not maintain Routing Information.
→ 2 Phases: (i) Route Discovery: determines the most optimal path for transmission of data packets blw source & destination.
(ii) Route Maintenance: Performs maintenance. Looks after link breakage, nlw failure, etc.

(b) Adhoc on demand Vector Routing Protocol (AODV).
→ Extension of Dynamic Source Routing Protocol.
→ In DSR, the Mobile node contains complete path in its header.
→ As Nlw size increases, length of Path ↑, header size ↑ which makes the whole nlw slow.
→ Solution is Ad hoc on Demand Vector Routing Protocol.
→ AODV source node does not store complete path info, each node stores info of its previous & next node.
→ 2 Phases → Route Discovery & Route Maintenance.

(3) Hybrid Routing Protocols:
→ Combines the advantages of both reactive & Pro active RP.
→ Adaptive in nature and adapts according to the zone and position of source & destination nodes.
→ Zone Routing Protocol (ZRP). Whole nlw is divided into zones and position of source & destination node is observed.
→ If source & dest. node are in same zone, proactive R.A is used.
→ If they are in different zones, reactive R.A is used.

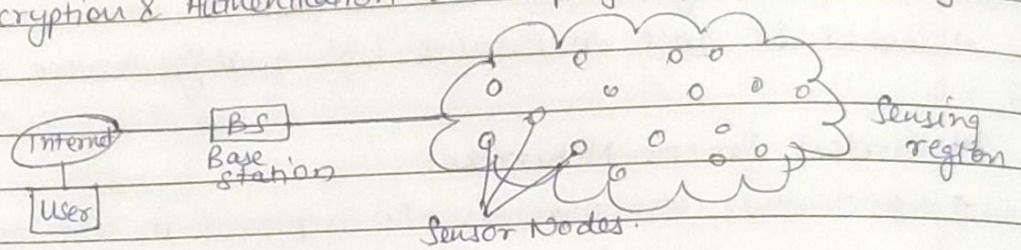
(*) Characteristics of MANET:

→ Should be widely distributed.
→ Must be localized.
→ Because of Mobility, it should be able to adjust frequent changes in N/w topology.
→ Must be free of impermeable routes.
→ Convergence of routes must be fast.
→ Should be able to provide high quality service.

(*) Wireless Sensor Networks:

→ Infrastructure less wireless n/w deployed in large no. of wireless sensors in an adhoc manner.
→ A n/w of spatially distributed autonomous sensors that are equipped with sensors to monitor physical or environmental conditions. to transmit data wirelessly to a central location.
→ Have gained significant importance due to the ability to provide real time data & control in harsh environments.
→ Sensor nodes are connected to a base station which acts as processing unit in WSN environment/System.
→ Base station is connected through internet to share data.
→ WSN can be used for processing, analysis, storage & mining of data.
→ Sensor nodes communicate with each other with a central base station.
→ This wireless communication can be achieved using zigbee, IEEE 802.15.4, wifi, etc.
→ WSNs have different topologies, including star, tree, mesh, adhoc n/w.
→ Choice of topology depends upon application & requirements.
→ Sensor nodes collect data from environment and transmit them

to a central data collection point
→ Sensor nodes are typically battery powered & have limited energy resources.
→ Advanced nodes have more powerful processors for complex tasks.
→ WSNs must be secured to protect against data breaches & unauthorized access.
→ Encryption & Authentication are employed for confidentiality & integrity.



(*) Components of WSN:
① Sensors: Used to capture the environmental variables which are used for data acquisition.
Sensor signals are converted to electrical signals.
② Sensor nodes: fundamental building blocks of WSN. Each node includes a sensor, processing unit, memory & transceiver.
③ Radio Nodes: Used to receive data produced by sensors and sends it to WLAN access point.
④ WLAN Access Point: Receives the data sent by Radio Nodes.
⑤ Evaluation Software: Data received by WLAN access point is evaluated by this software for presenting the report to users.

(*) Applications of WSN:
① Internet of Things (IOT)
② Monitor for security, threat detection.
③ Environmental temperature, Humidity, air pressure.
④ Noise level.
⑤ Medical Applications, detection of Earthquakes, landslides, etc.

(*) Challenges of WSN:

1. Quality of service
2. Security Issue
3. Energy Efficiency
4. NW throughput
5. Performance
6. Ability to cope with node failure
7. Scalability
8. Limited Power & Energy.
9. Limited Processing & storing capabilities (Difficulty in complex tasks).
10. It consists of a variety of different sensor types that is challenging.
11. They are often deployed in environments where there is a lot of interference from other wireless devices.

(*) Advantages:

1. Low cost
2. Wireless Communication.
3. Energy Efficiency
4. Can be scaled up/down easily.
5. Real time monitoring.

(*) Disadvantages:

1. Limited Range
2. Limited Processing Power
3. Data security.
4. Interference
5. Deployment challenges.

(*) RFID Technology: (Radio frequency IDentification).

→ Uses radio waves to passively identify a tagged object.
→ Used in several commercial and industrial applications.
→ Eg. Tracking items along a supply chain, tracking items checked out of a library.
→ 2 components: tags and readers.
→ Reader is a device that has one or more antennas and that emit radio waves and receive signals back from RFID tag.
→ Tags can be active or passive.
→ Passive RFID tags are powered by reader & do not have any battery. Active RFID tags are powered by batteries.
→ Can store info. from one serial no. to several pages of data.
→ Readers can be mobile so that they can be carried.
→ It is used in conjunction with a microchip, a powered antenna

and a scanner.
→ It is now more affordable to purchase and adopt
→ Microchip has info stored on it.
→ Small devices that can hold large amounts of data.
→ Microchips don't emit electricity. Some can contain a stored power source or batteries.
→ Scanners can also provide enough electricity to allow them to read a microchip.
→ Commonly used in tracking products, animals & currency.

(v). Uses:
In hospitals: Inventory control, Equipment tracking, Out-of-bed detection & fall detection, Ensuring patients receive correct medications & medical devices, monitoring patients, Providing data for Medical records.

(vi). Wifi Standards: (Stands for wireless fidelity).
→ Each wifi nlw standard has 2 parameters:
① Speed: Data transfer rate of nlw (in Mbps)
② Frequency: On what frequency the nlw is carried on.
→ Single Band Routers: 2.4 GHz OR 5 GHz frequency.
→ Dual-band Routers: 2.4 GHz AND 5 GHz frequency.
→ 2.4 GHz is used by many devices, so the signal becomes overcrowded & speed becomes slow. Solution → 5 GHz.
→ 5 GHz has faster rate but less range than 2.4 GHz.

(vii). Different Standards of wifi:
① IEEE 802.11 → Speed is about 2 Mbps.
② IEEE 802.11a – Useful for commercial & industrial purposes.
→ works on 5 GHz frequency.
→ Max. speed is 54 Mbps. (1999)
→ Made to avoid interference with other devices which use 2.4 GHz band.

② IEEE 802.11b - created with 802.11a. (1999)
→ It uses 2.4 GHz frequency band.
→ Speed is 11 Mbps.
→ Used for Home & domestic use.
③ IEEE 802.11g : (2003) Max speed - 54 Mbps.
→ Has combined properties of 802.11a & 802.11b.
→ Frequency band used is 2.4 GHz for better coverage.
④ IEEE 802.11n : (2009) Max speed = 600 mbps.
→ Operates on both 2.4 GHz & 5 GHz bands, but individually.
⑤ IEEE 802.11ac : (2013) Max speed - 1.3 Gbps.
→ Works on 5 GHz band.
⑥ IEEE 802.11ax : Newest & advanced version of wifi (2019)
→ Operates on both the bands for better coverage & better speed.
→ Max speed = 10 gbps.
⑦ New Naming standards: 802.11b → Wifi 1, 802.11a → Wifi 2, 802.11g → Wifi 3, 802.11n → Wifi 4, 802.11ac → Wifi 5, 802.11ax → Wifi 6.

(*) WiMax Standards: Wireless broadband communication technology.
→ Provides high speed data over wide area.
→ Stands for worldwide Interoperability for Microwave Access.
→ Able to meet the needs of a large variety of users.
→ High speed data network, very cheap, less installation time.
→ Aims to provide wireless broadband services with a target range of upto 31 miles & rate exceeding 100 Mbps.
→ IEEE 80.16 and WiMax are used interchangeably.
→ WiMax is to IEEE 802.16 what Wifi is to IEEE 802.11
→ A standard for wireless Metropolitan Area Network (WMAN)
→ Uses some key technologies to enable it to provide high speed data rates:

(a). OFDM (Orthogonal Frequency Division Multiplex): To provide high speed data without selective fading.

(b). MIMO (Multiple Input Multiple Output): Makes use of multipath propagation.

Use of MIMO either enables operations with lower signal strength levels or allows for higher data rates.

→ WiMAX currently includes 802.16-2004 & 802.16e

→ 802.16-2004 utilizes OFDM to serve multiple users in a time division fashion is a sort of round robin technique.

→ It is done so quickly that the users have the perception that they are always transmitting / receiving data.

→ OFDM can serve multiple users simultaneously.

(c). Fem to Cell Network: Femtocell / Femto Nw.

→ Small, low powered & short range cellular base station designed to enhance cellular coverage and capacity in localized areas.

→ Typically used in residential / small business settings to improve indoor cellular coverage, reduce Nw congestions & traffic.

→ Powered by a mobile Nw operator and operates in licensed frequency bands.

→ Used to provide Nw coverage to the devices where macrocells cannot reach or have weak coverage.

→ Features:

① Small coverage Area: A few meters to a few hundered meters.

② Home use: Acts as a miniature cellular base station.

③ Offloading: Offload cellular traffic from macrocellular Nw.

→ When a mobile device is in coverage of femto cell, it connects to femtocell instead of distant macrocell.

④ Internet Connectivity: Require Internet connection (Wired or wireless).

⑤ Security and Authentication: Only authorized users can connect.
⑥ Managed by Mobile Operators: They control Nlw configuration, security and access to femtocell.
⑦ Interference Mitigation: minimize interference.
⑧ Voice & Data: Support both voice & data services.
⑨ Fast data speed. Useful in areas with poor cellular coverage.

→ The main difference blw a femto cell, base station, microcell or picocell is the range.
→ Base station range: 20-30 km, macro cell - 1-2 km, picocell - 200-300 m, femto cell - as low as 10m.
→ Can switch blw femto cell & macrocell according to signal strength
→ Plug-and-play devices. Require no seperate installation.
→ Only allow pre declared phone numbers to connect with it.
→ Also have protection mechanism and report changes in location to MNO (Mobile Nlw Operator).

(v) Advantages:
① Exceptional coverage.
② Better voice Quality
③ Less power use (Improves Battery).
④ Provide higher mobile data capacity

(vi) Disadvantages:
① Uses same frequency band as conventional Nlw, may cause interference.
② Femto cells may affect the quality of service in shared bandwidth scenarios.
③ Problems may arise when provider of broadband service differs from Mobile Network Operator.

→ Effective solutions for addressing "dead zones".

(vii) Push to talk technology: (PTT)
→ A two way communication method that allows users to have instant voice conversations by pressing a button or

activating a virtual switch.

→ Commonly associated with walkie-talkie devices & radio communication systems.

→ Primarily used for voice conversations, there isn't a direct equivalent for SMS (text messaging) as PTT is designed for real time voice communication.

(*) Features:

① Instant Messaging Apps: Many apps offer "voice message" feature. Allows users to record a short voice message and send it to their contacts.
Quick and convinient way.

② Voice Messages in Text chats: Some messaging apps allow users to send voice messages within a text chat. You can record a short message and send it and recipient can play it back when they have time.

③ Group Chat: similar to PTT group conversation. Multiple users can participate in single chat. Messages are sent in real time.

④ Enterprise solutions: There are communication and collaboration tools that offer text messaging, voice messaging, video conferencing, etc.

→ These features offer a way to communicate quickly with voice or text & they can be very useful for various scenarios.

(*) VANET: Vehicular Ad hoc NWs.

→ similar to MANET

→ plays an important role in aspects of safe driving, intelligent navigation, emergency applications, etc.

→ Vehicles are able to communicate with each other as well as roadside Base stations located at critical points on the road.

(*) Uses:

① Intelligent transportation System Used to enhance traffic flow, reduce congestion & improve road safety.

② Navigation & location-based services: Provides real time traffic and navigation information to drivers allowing them to make informed decisions.

③ Emergency services: Can be used to quickly & efficiently relay emergency messages such as accidents, road closures, etc.

④ Vehicle to Vehicle (V2V) & Vehicle to Infrastructure (V2I) communications: facilitate communication for cooperative driving.

⑤ Entertainment and Infotainment Services: Allows streaming music and video for passengers in vehicles.

(*) Communication in VANET: 3 Types:

① Vehicle to Vehicle (V2V): Vehicles, within a communication range exchange data with the help of a wireless nlw.

→ Data exchanged includes speed, location, direction, traffic information, driver behaviour, road condition & other useful information. Range can be upto 300m.

→ Makes Vehicles Smarter, leading to Intelligent Transport Systems (ITS).

② Vehicle to Infrastructure (V2I): Comm. b/w vehicles & roadside Infrastructure (traffic junctions, roadside Access Points, etc).

→ Avoid Motor crashes, ambulance assistance, etc.

→ There is a Need for applications that combine V2V & V2I for efficiency & safety.

③ Inter-Infrastructure Comm. (I2I): Road side Infrastructure communicate with each other to achieve a wider range.

→ Offers greater flexibility in content sharing & range is increased by offering multi-hop communication. Gives rise to a Hybrid VANET architecture to enable seamless connectivity.