UNIT-5

IEEE 802.11: IEEE 802.11 standard, popularly known as WiFi, lays down the architecture and specifications of wireless LANs (WLANs). WiFi or 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.

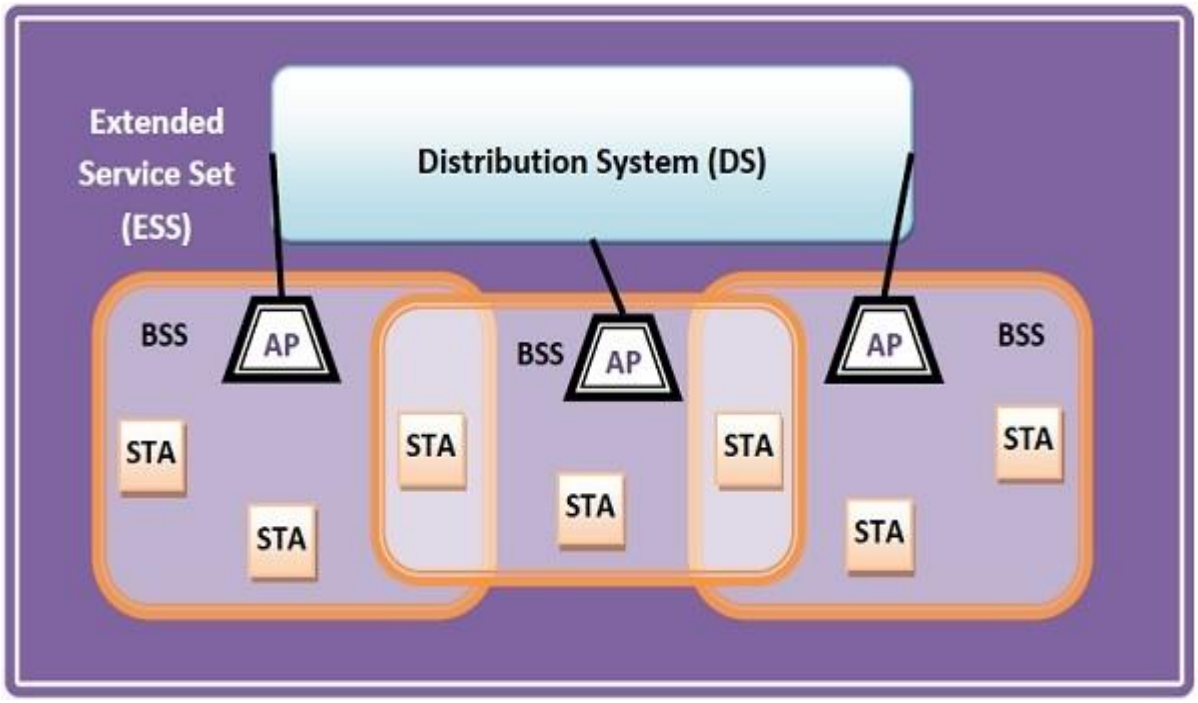
IEEE 802.11 Architecture

The components of an IEEE 802.11 architecture are as follows −

- **Stations (STA)** − Stations comprises of all devices and equipment that are connected to the wireless LAN. A station can be of two types−
    - Wireless Access Point (WAP) − WAPs or simply access points (AP) are generally wireless routers that form the base stations or access.
    - Client. Clients are workstations, computers, laptops, printers, smartphones, etc.

  Each station has a wireless network interface controller.
- **Access Point (AP):** An Access Point is a central device that connects wireless clients (STAs) to a wired network. It acts as a bridge between wireless and wired networks, allowing wireless devices to access resources on the wired network.
- **Basic Service Set (BSS)** − A basic service set is a group of stations communicating at the physical layer level. BSS can be of two categories depending upon the mode of operation−
    - Infrastructure BSS − Here, the devices communicate with other devices through access points.
    - Independent BSS − Here, the devices communicate in a peer-to-peer basis in an ad hoc manner.
- **Extended Service Set (ESS)** - An ESS is a collection of interconnected BSSs. It allows users to roam seamlessly between different BSSs within the same ESS while maintaining their network connection
- **Distribution System (DS)** − The Distribution System is responsible for interconnecting multiple BSSs and allows for the exchange of data between them. It ensures seamless roaming and network-wide communication

.



Services: IEEE 802.11 networks provide various services, including authentication and association services for connecting STAs to an AP, distribution services for managing data distribution, and integration services for connecting wireless networks to wired networks.

Frequency Bands: IEEE 802.11 networks operate in various frequency bands, including 2.4 GHz and 5 GHz bands, with different standards like 802.11b, 802.11a, 802.11g, and 802.11n. Each standard defines the modulation and data rates for wireless communication.

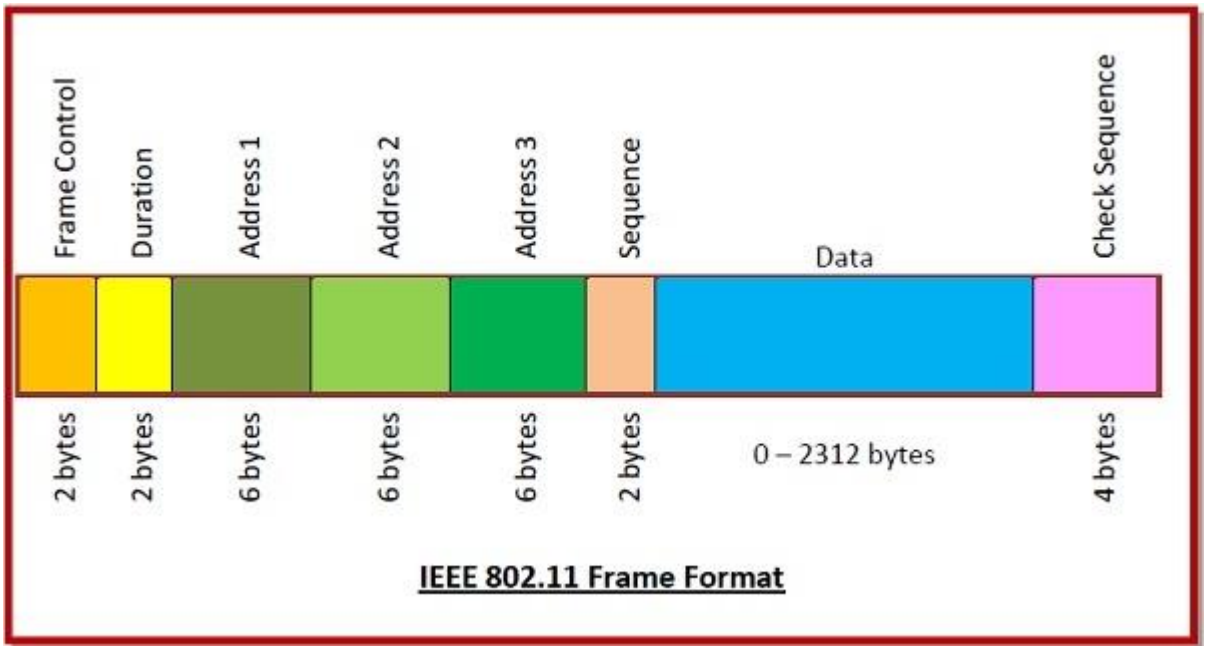
Security: IEEE 802.11 includes various security mechanisms, such as WEP, WPA, and WPA2/WPA3, to protect wireless communication from unauthorized access and eavesdropping.

Frame Format of IEEE 802.11

The main fields of a frame of wireless LANs as laid down by IEEE 802.11 are −

- **Frame Control** − It is a 2 bytes starting field composed of 11 subfields. It contains control information of the frame.
- **Duration** − It is a 2-byte field that specifies the time period for which the frame and its acknowledgment occupy the channel.
- **Address fields** − There are three 6-byte address fields containing addresses of source, immediate destination, and final endpoint respectively.
- **Sequence** − It a 2 bytes field that stores the frame numbers.

- **Data** − This is a variable-sized field that carries the data from the upper layers. The maximum size of the data field is 2312 bytes.
- **Check Sequence** − It is a 4-byte field containing error detection information.



IEEE 802.11 Protocol Architecture: The IEEE 802.11 protocol architecture is a comprehensive framework that governs various aspects of wireless communication, from hardware specifications to network management and security. Different versions of the standard, such as 802.11b, 802.11g, 802.11n, and more, have introduced improvements and enhancements to this architecture over the years to meet evolving wireless networking needs. The architecture is organized into several layers, similar to the OSI model:

1. **Physical** Layer (PHY): The PHY layer deals with the physical aspects of wireless communication. It defines the modulation techniques, frequency bands, data rates, and other hardware-related parameters. Different IEEE 802.11 standards (e.g., 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, etc.) specify various PHY layers with different characteristics.
2. **Logical Link Control (LLC):** The LLC sublayer sits between the MAC layer and the upper layers and provides a common interface for multiple higher-layer protocols. It is responsible for link management and encapsulation. Its primary functions include:

- **Frame Addressing and Identification:** The LLC sublayer assigns a unique address to each frame, allowing devices to identify and process the frames that are intended for them. It uses source and destination MAC addresses in the frame header to determine the source and destination of data frames.
- **Frame Multiplexing:** The LLC sublayer enables the multiplexing of data from various network layer protocols. It allows multiple higher-layer protocols (e.g., IP, IPX, IPv6) to share the same physical medium.
- **Error Detection and Control**: The LLC sublayer is responsible for error detection and correction. It adds error-checking information (such as Frame Check Sequence or FCS)

to frames, enabling the receiver to detect and possibly correct errors in the received data.

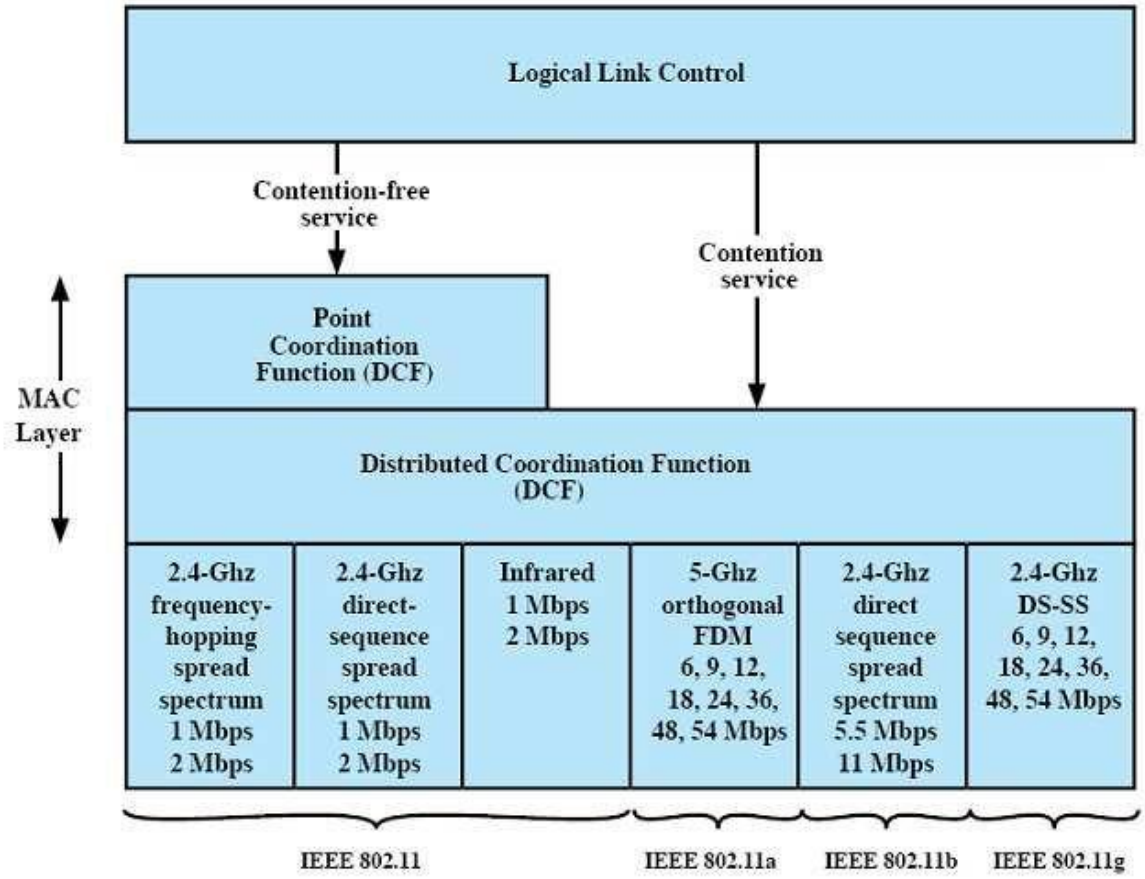
- **Flow Control:** LLC can be involved in flow control mechanisms to manage the rate at which frames are transmitted between devices. Flow control is essential to prevent network congestion and ensure efficient data transmission.
- **Frame Control and Management**: The LLC sublayer handles various control frames that are used for network management, such as frame acknowledgment and frame retransmission. These control frames are essential for maintaining the reliability of data transmission.
- **Frame Format and Encapsulation**: The LLC sublayer defines the format in which data frames are encapsulated. It specifies how data from higher-layer protocols is packaged into frames, including how headers, trailers, and data payloads are structured.

3. **Medium Access Control (MAC):** The MAC layer manages access to the shared wireless medium, coordinating how devices contend for the right to transmit data. It includes functions like frame management, addressing, error checking, and fragmentation. The MAC layer serves as the bridge between the higher-layer protocols and the physical layer, ensuring that data is transmitted efficiently and reliably in a shared wireless environment. It plays a critical role in managing the complexities of wireless communication and is an integral part of the IEEE 802.11 standard. Different IEEE 802.11 standards may introduce variations and enhancements to the MAC layer to improve performance, security, and features.

   MAC layer provides functionality for several tasks like control medium access, can also offer support for roaming, authentication, and power conservation. The basic services provided by MAC are the mandatory asynchronous data service and optional time-bounded service. IEEE 802.11 defines two MAC sub-layers:-

   Distributed Coordination Function (DCF) – DCF uses CSMA/CA as access method as wireless LAN can't implement CSMA/CD. It only offers asynchronous service.

   Point Coordination Function (PCF) – PCP is implemented on top of DCF and mostly used for time-service transmission. It uses a centralized, contention-free polling access method. It offers both asynchronous and time-bounded service.



HIPERLAN: HIPERLAN stands for **high performance local area network**. It is a wireless standard derived from traditional LAN environments and can support multimedia and asynchronous data effectively at high data rates of 23.5 Mbps. It is primarily a European standard alternative for the IEEE 802.11 standards and was published in 1996. It is defined by the European Telecommunications Standards Institute (ETSI). It does not necessarily require any type of access point infrastructure for its operation, although a LAN extension via access points can be implemented. Radio waves are used instead of a cable as a transmission medium to connect stations. Either, the radio transceiver is mounted to the movable station as an add-on and no base station has to be installed separately, or a base station is needed in addition per room. The stations may be moved during operation-pauses or even become mobile. The maximum data rate for the user depends on the distance of the communicating stations. With short distance(<50 m) and asynchronous transmission a data rate of 20 Mbit/s is achieved, with up to 800 m distance a data rate of 1 Mbit/s are provided. For connection-oriented services, e.g. video-telephony, at least 64 kbit/s are offered.

HIPERLAN uses cellular-based data networks to connect to an ATM backbone. The main idea behind HIPERLAN is to provide an infrastructure or ad-hoc wireless with low mobility and a small radius. HIPERLAN supports isochronous traffic with low latency. The HiperLAN standard family has four different versions. The key feature of all four networks is their integration of time-sensitive data transfer services. Over time, names have changed and the

former HIPERLANs 2,3, 1nd 4 are now called HiperLAN2, HIPERACCESS, and HIPERLINK.

Table 2.1: HIPERLAN protocol family

	HIPERLAN 1	HIPERLAN 2	HIPERLAN 3	HIPERLAN 4
Application	wireless LAN	access to ATM fixed networks	wireless local loop	point-to-point wireless ATM connections
Frequency	5.1-5.3GHz			17.2-17.3GHz
Topology	decentralized ad-hoc/infrastructure	cellular, centralized	point-to-multipoint	point-to-point
Antenna	omni-directional		directional	
Range	50 m	50-100 m	5000 m	150 m
QoS	statistical	ATM traffic classes (VBR, CBR, ABR, UBR)		
Mobility	<10m/s		stationary	
Interface	conventional LAN	ATM networks		
Data rate	23.5 Mbit/s	>20 Mbit/s		155 Mbit/s
Power conservation	yes		not necessary	

1. **HIPERLAN 1:** Planning for the first version of the standard, called HiperLAN/1, started 1991, when planning of 802.11 was already going on. The goal of the HiperLAN was the high data rate, higher than 802.11. The standard was approved in 1996. The functional specification is EN300652, the rest is in ETS300836. The standard covers the Physical layer and the Media Access Control part of the Data link layer like 802.11. There is a new sub layer called Channel Access and Control sub layer (CAC). This sub layer deals with the access requests to the channels. The accomplishing of the request is dependent on the usage of the channel and the priority of the request. CAC layer provides hierarchical independence with Elimination-Yield Non-Preemptive Multiple Access mechanism (EY-NPMA). EY-NPMA codes priority choices and other functions into one variable length radio pulse preceding the packet data. EY-NPMA enables the network to function with few collisions even though there would be a large number of users. Multimedia applications work in HiperLAN because of EY-NPMA priority mechanism. MAC layer defines protocols for routing, security and power saving and provides naturally data transfer to the upper layers. On the physical layer FSK and GMSK modulations are used in HiperLAN/1. HiperLAN features:
    - range 50 m
    - slow mobility (1.4 m/s)
    - supports asynchronous and synchronous traffic

- sound 32 kbit/s, 10 ns latency
- video 2 Mbit/s, 100 ns latency
- data 10 Mbit/s

2. **HiperLAN Type 2:** Next generation of HiperLAN family: Proposed by ETSI BRAN (Broadband Radio Access Networks) in 1999, and is still under development.

   Goal: Providing high-speed (raw bit rate ~54Mbps) communications access to different broadband core networks and moving terminals

   Features: connection-oriented, QoS guaranteed, security mechanism, highly flexibility

   Product: Prototypes are available now, and commercial products are expected at the end of 2001 (Ericsson).

3. **HiperAccess and HiperLink:** In parallel to developing the HIPERLAN Type 2 standards, ETSI BRAN has started work on standards complementary to HIPERLAN Type 2

Bluetooth: It is a network technology that connects mobile devices wirelessly over a short-range to form a personal area network (PAN). They use short-wavelength, ultra-high frequency (UHF) radio waves within the range 2.400 to 2.485 GHz, instead of RS-232 data cables of wired PANs.

Features of Bluetooth

- Bluetooth technology was released in 1999 as Bluetooth 1.0, by Special Interest Group (SIG) who continues to manage it.
- It was initially standardized as IEEE 802.15.1.
- Mobile computing devices and accessories are connected wirelessly by Bluetooth using short-range, low-power, inexpensive radios.
- UHF radio waves within the range of 2.400 to 2.485 GHz are using for data communications.
- A PAN or a piconet can be created by Bluetooth within a 10 m radius.
- Presently, 2 to 8 devices may be connected.
- Bluetooth protocols allow devices within the range to find Bluetooth devices and connect with them. This is called pairing. Once, the devices are paired, they can transfer data securely.
- Bluetooth has lower power consumption and lower implementation costs than Wi-Fi. However, the range and transmission speeds are typically lower than Wi-Fi.
- The lower power requirements make it less susceptible to interference with other wireless devices in the same 2.4GHz bandwidth.
- Bluetooth version 3.0 and higher versions can deliver a data rate of 24 Mbps.

- The Bluetooth version 4.0 came in 2010. It is characterized by low energy consumption, multivendor interoperability, the economy of implementation, and greater range.

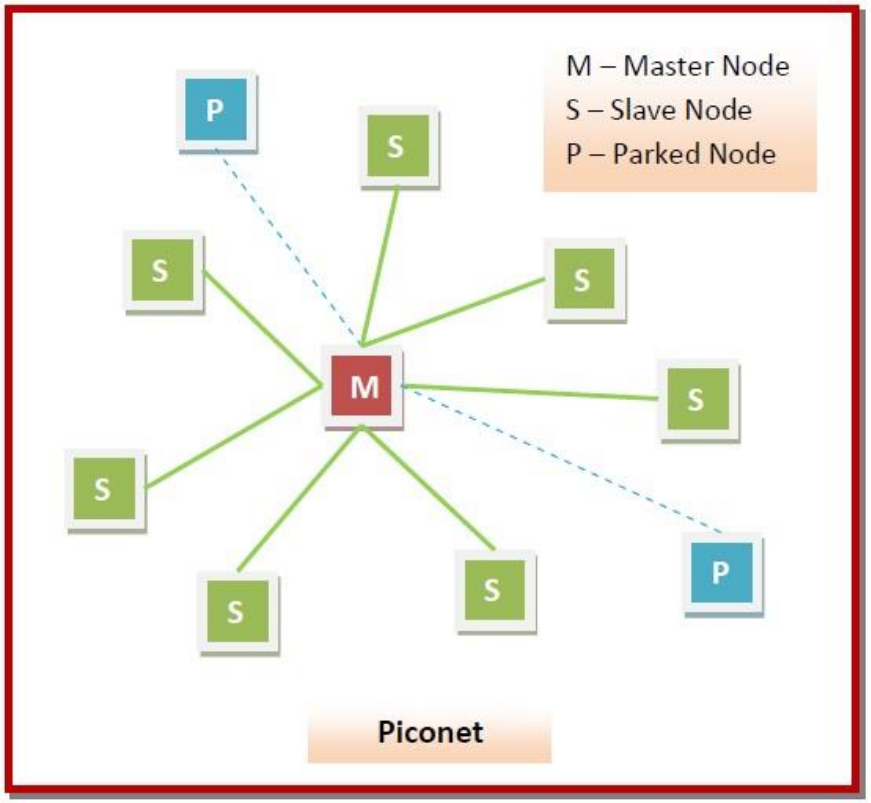
Bluetooth Architecture: Bluetooth is a network technology that connects mobile devices wirelessly over a short range to form a personal area network (PAN). They use short-wavelength, ultra-high frequency (UHF) radio waves within the range 2.400 to 2.485 GHz, instead of RS-232 data cables of wired PANs.

There are two types of Bluetooth networks −

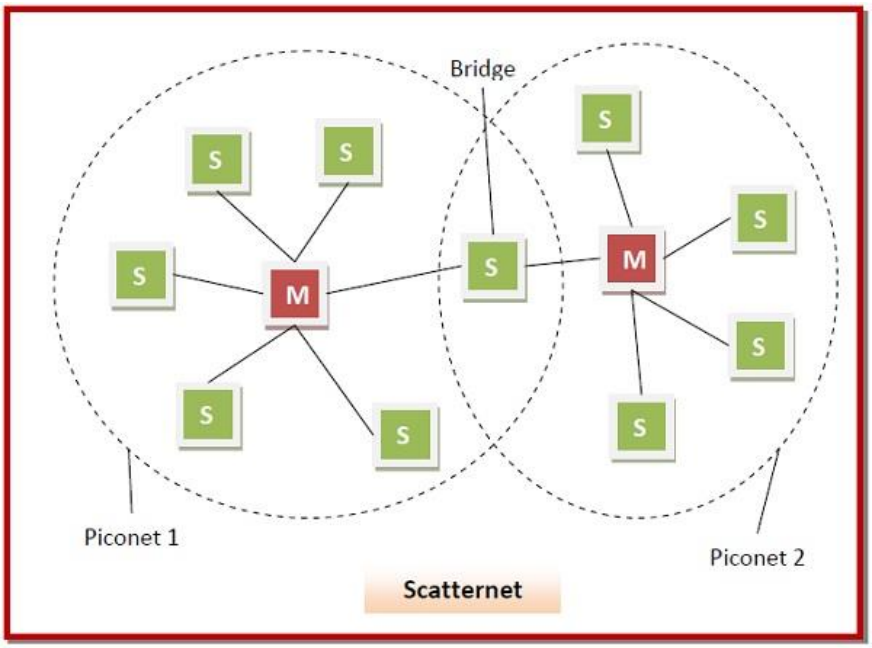
- Piconets
- Scatternets

Piconets: Piconets are small Bluetooth networks, formed by at most 8 stations, one of which is the master node and the rest slave nodes (maximum of 7 slaves). Master node is the primary station that manages the small network. The slave stations are secondary stations that are synchronized with the primary station. Communication can take place between a master node and a slave node in either one-to-one or one-to-many manner. However, no direct communication takes place between slaves. Each station, whether master or slave, is associated with a 48-bit fixed device address**.**

Besides the seven active slaves, there can be up to 255 numbers of parked nodes. These are in a low power state for energy conservation. The only work that they can do is respond to a beacon frame for activation from the master node.



Scatternets: A scatternet is an interconnected collection of two or more piconets. They are formed when a node in a piconet, whether a master or a slave, acts as a slave in another piconet. This node is called the bridge between the two piconets, which connects the individual piconets to form the scatternet. It offer the advantage of expanding the capabilities of Bluetooth networks by enabling more devices to communicate in complex environments. This concept allows for more flexible and scalable Bluetooth applications in a variety of scenarios. However, managing the coordination and interference between multiple piconets within a scatternet can be challenging and requires careful design and protocol management.



IEEE 802.15: IEEE 802.15.4 is a low-cost, low-data-rate wireless access technology for devices that are operated or work on batteries. This describes how low-rate wireless personal area networks (LR-WPANs) function. IEEE 802.15 is a working group within the Institute of Electrical and Electronics Engineers (IEEE) that focuses on developing standards for wireless personal area networks (WPANs). WPANs are typically designed for short-range, low-power wireless communication between devices, and they serve a variety of applications. The most well-known standard developed by the IEEE 802.15 working group is Bluetooth, but there are other standards within this group as well. Here are some of the key standards and specifications associated with IEEE 802.15:

IEEE 802.15.1 (Bluetooth): Bluetooth is one of the most widely recognized standards within the IEEE 802.15 family. It defines the specifications for short-range wireless communication between devices, such as smartphones, headphones, and IoT devices. Bluetooth operates in the 2.4 GHz ISM band and provides various profiles for different use cases, including audio streaming, data transfer, and more.

IEEE 802.15.4: IEEE 802.15.4 is a standard that specifies the physical (PHY) and medium access control (MAC) layers for low-rate wireless personal area networks. It is designed for low-power, low-data-rate, and low-complexity applications. IEEE 802.15.4 serves as the basis for various wireless communication standards, such as Zigbee, 6LoWPAN, and Thread.

IEEE 802.15.4a (UWB): This standard extends IEEE 802.15.4 by adding support for ultra-wideband (UWB) communication. UWB allows for precise location and tracking applications and is used in applications like Real-Time Location Systems (RTLS) and asset tracking.

IEEE 802.15.4g (Smart Utility Networks): This standard is designed for smart utility networks, particularly in the context of smart grid applications. It defines the physical and MAC layer specifications for wireless communication in this context.

IEEE 802.15.4e (Time-Synchronized Channel Hopping): IEEE 802.15.4e is an amendment to the IEEE 802.15.4 standard that introduces time-synchronized channel hopping (TSCH). TSCH is a method for improving the reliability and determinism of wireless communication in industrial and critical infrastructure applications. The 802.15.4e improves the old standard by introducing mechanisms such as time slotted access, multichannel communication and channel hopping.

IEEE 802.15.5 (Mesh Networking): This standard defines the architecture and protocols for wireless mesh networking in WPANs. Mesh networks allow devices to relay data through intermediate nodes, enhancing network coverage and robustness.

IEEE 802.15.6 (Body Area Networks): This standard focuses on wireless communication between devices located on or around the human body, often referred to as Body Area Networks (BANs). It is used in medical and healthcare applications, such as wearable health monitoring devices.

IEEE 802.15.7 (Visible Light Communication): IEEE 802.15.7 defines standards for visible light communication (VLC), where data is transmitted using visible light. This technology is often used for indoor positioning and communication, particularly in scenarios where radio frequency communication is not suitable.

These IEEE 802.15 standards cover a wide range of wireless communication technologies, each tailored to specific use cases and application domains. They enable a variety of short-range wireless connectivity options for personal area networks, industrial IoT, healthcare, smart grid, and more.

IEEE 802.15.4e introduces the following general functional enhancements:

1. Low Energy (LE): This mechanism is intended for applications that can trade latency for energy efficiency. It allows a node to operate with a very low duty cycle.

2. **Information Elements (IE):** It is an extensible mechanism to exchange information at the MAC sublayer.

3. **Enhanced Beacons (EB):** Enhanced Beacons are an extension of the 802.15.4 beacon frames and provide a greater flexibility. They allow to create application-specific frames.

4. **Multipurpose Frame:** This mechanism provides a flexible frame format that can address a number of MAC operations. It is based on IEs.

5. **MAC Performance Metric:** It is a mechanism to provide appropriate feedback on the channel quality to the networking and upper layers, so that appropriate decision can be taken.

6. **Fast Association (FastA):** The 802.15.4 association procedure introduces a significant delay in order to save energy. For time-critical application latency has priority over energy efficiency.

- IEEE 802.15.4e defines five new MAC behavior modes:

1. **Time Slotted Channel Hopping (TSCH):** It targets application domains such as industrial automation and process control, providing support for multi-hop and multichannel communications, through a TDMA approach.

2. **Deterministic and Synchronous Multi-channel Extension (DSME):** It is aimed to support both industrial and commercial applications.

3**. Low Latency Deterministic Network (LLDN):** Designed for single-hop and single channel networks

4. **Radio Frequency Identification Blink (BLINK):** It is intended for application domains such as item/people identification, location and tracking.

5. **Asynchronous multi-channel adaptation (AMCA):** It is targeted to application domains where large deployments are required, such as smart utility networks, infrastructure monitoring networks, and process control networks.

Properties:

1. Standardization and alliances: It specifies low-data-rate PHY and MAC layer requirements for wireless personal area networks (WPAN). IEEE 802.15. Protocol Stacks include:

- **ZigBee:** ZigBee is a Personal Area Network task group with a low rate task group 4. It is a technology of home networking. ZigBee is a technological standard created for controlling and sensing the network. As we know that ZigBee is the Personal Area network of task group 4 so it is based on IEEE 802.15.4 and is created by Zigbee Alliance.
- **6LoWPAN:** The 6LoWPAN system is used for a variety of applications including wireless sensor networks. This form of wireless sensor network sends data as packets and uses IPv6 – providing the basis for the name – IPv6 over Low power Wireless Personal Area Networks.
- **ZigBee IP:** Zigbee is a standards-based wireless technology that was developed for low-cost and low-power wireless machine-to-machine (M2M) and internet of things (IoT) networks.
- **ISA100.11a:** It is a mesh network that provides secure wireless communication to process control.
- **Wireless HART:** It is also a wireless sensor network technology, that makes use of time-synchronized and self-organizing architecture.
- **Thread:** Thread is an IPv6-based networking protocol for low-power Internet of Things devices in IEEE 802.15. 4-2006 wireless mesh network. Thread is independent.

2. Physical Layer: This standard enables a wide range of PHY options in ISM bands, ranging from 2.4 GHz to sub-GHz frequencies. IEEE 802.15.4 enables data transmission speeds of 20 kilobits per second, 40 kilobits per second, 100 kilobits per second, and 250 kilobits per second. The fundamental structure assumes a 10-meter range and a data rate of 250 kilobits per second. To further reduce power usage, even lower data rates are possible. IEEE 802.15.4

regulates the RF transceiver and channel selection, and even some energy and signal management features, at the physical layer. Based on the frequency range and data performance needed, there are now six PHYs specified. Four of them employ frequency hopping techniques known as Direct Sequence Spread Spectrum (DSSS). Both PHY data service and management service share a single packet structure so that they can maintain a common simple interface with MAC.

3. MAC layer: The MAC layer provides links to the PHY channel by determining that devices in the same region will share the assigned frequencies. The scheduling and routing of data packets are also managed at this layer. The 802.15.4 MAC layer is responsible for a number of functions like:

- Beaconing for devices that operate as controllers in a network.
- used to associate and dissociate PANs with the help of devices.
- The safety of the device.
- Consistent communication between two MAC devices that are in a peer-to-peer relationship.

Several established frame types are used by the MAC layer to accomplish these functions. In 802.15.4, there are four different types of MAC frames:

- frame of data
- Frame for a beacon
- Frame of acknowledgement
- Frame for MAC commands
-

4. Topology: Networks based on IEEE 802.15.4 can be developed in a star, peer-to-peer, or mesh topology. Mesh networks connect a large number of nodes. This enables nodes that would otherwise be out of range to interact with each other to use intermediate nodes to relay data.

5. Security: For data security, the IEEE 802.15.4 standard employs the Advanced Encryption Standard (AES) with a 128-bit key length as the basic encryption technique. Activating such security measures for 802.15.4 significantly alters the frame format and uses a few of the payloads. The very first phase in activating AES encryption is to use the Security Enabled field in the Frame Control part of the 802.15.4 header. For safety, this field is a single bit which is assigned to 1. When this bit is set, by taking certain bytes from its Payload field, a field known as the Auxiliary Security Header is formed following the Source Address field.

6. Competitive Technologies: The IEEE 802.15.4 PHY and MAC layers serve as a basis for a variety of networking profiles that operate in different IoT access scenarios. DASH7 is a competing radio technology with distinct PHY and MAC layers.

Advantages of IEEE 802.15.4: IEEE 802.15.4 has the following advantages:

- cheap cost
- long battery life,
- Quick installation
- simple
- extensible protocol stack

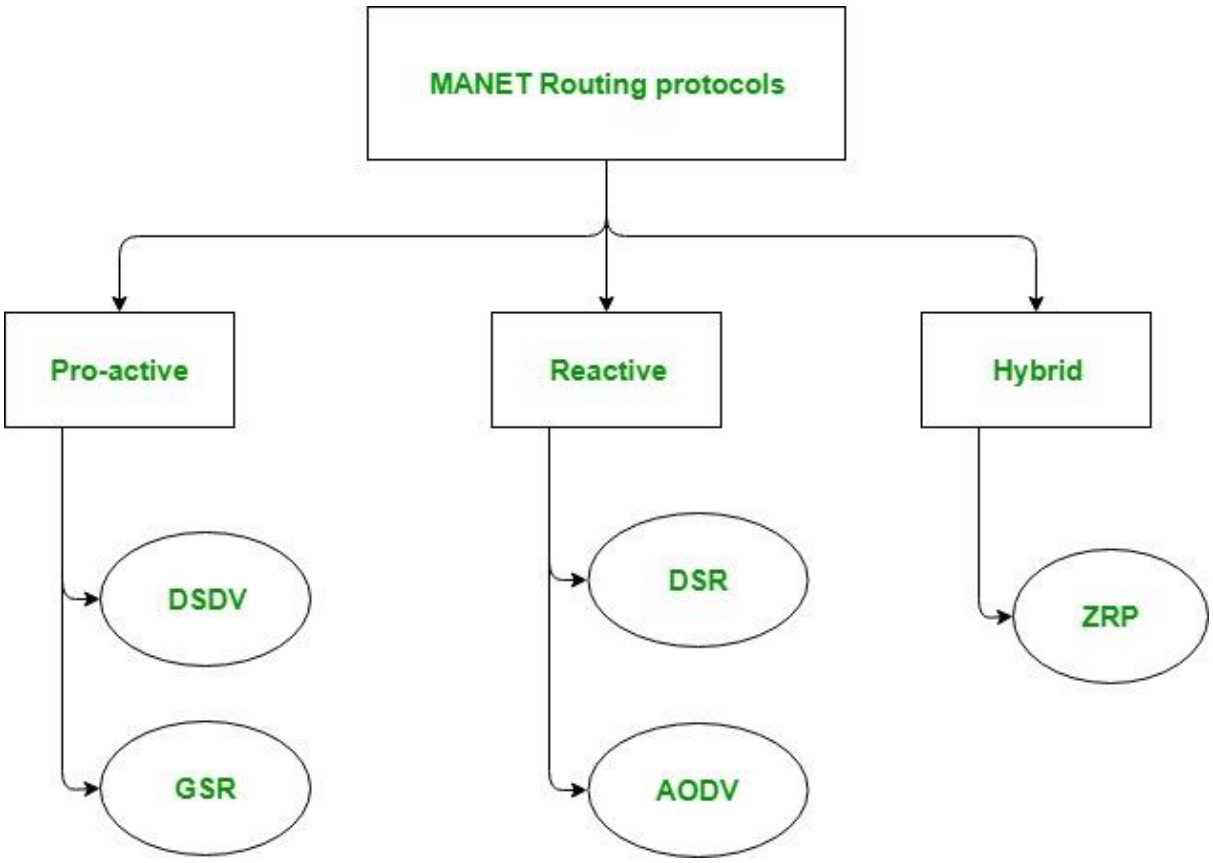
Disadvantages of IEEE 802.15.4: IEEE 802.15.4's drawbacks include:

- IEEE 802.15.4 causes interference and multipath fading.
- doesn't employ a frequency-hopping approach.
- unbounded latency
- interference susceptibility

Applications of IEEE 802.15.4: IEEE 802.15.4 Applications:

- Wireless sensor networks in the industry
- Building and home automation
- Remote controllers and interacting toys
- Automotive networkss

MANET characteristics ROUTING: In Mobile Ad hoc Network (MANET), nodes do not know the topology of their network, instead they have to discover it by their own as the topology in the ad-hoc network is dynamic topology. The basic rules is that a new node whenever enters into an ad-hoc network, must announce its arrival and presence and should also listen to similar announcement broadcasts made by other mobile nodes.



1. **Pro-active routing protocols:** These are also known as table-driven routing protocols. Each mobile node maintains a separate routing table which contains the information of the routes to all the possible destination mobile nodes.

Since the topology in the mobile ad-hoc network is dynamic, these routing tables are updated periodically as and when the network topology changes. It has a limitation that it doesn't work well for the large networks as the entries in the routing table becomes too large since they need to maintain the route information to all possible nodes.

i) Destination Sequenced Distance Vector Routing Protocol (DSDV): It is a pro-active/table driven routing protocol. It actually extends the distance vector routing protocol of the wired networks as the name suggests. It is based on the Bellman-ford routing algorithm. Distance vector routing protocol was not suited for mobile ad-hoc networks due to count-to-infinity problem. Hence, as a solution Destination Sequenced Distance Vector Routing Protocol (DSDV) came into picture.
Destination sequence number is added with every routing entry in the routing table maintained by each node. A node will include the new update in the table only if the entry consists of the new updated route to the destination with higher sequence number.

ii) Global State Routing (GSR): It is a pro-active/table driven routing protocol. It actually extends the link state routing of the wired networks. It is based on the Dijkstra's routing algorithm. Link state routing protocol was not suited for mobile ad-hoc networks because in it, each node floods the link state routing information directly into the whole network i.e. Global flooding which may lead to the congestion of control packets in the network.
Hence, as a solution Global State Routing Protocol (GSR) came into the picture. Global state routing doesn't flood the link state routing packets globally into the network. In GSR, each of the mobile node maintains one list and three tables namely, adjacency list, topology table, next hop table and distance table.

2. Reactive routing protocols: These are also known as on-demand routing protocol. In this type of routing, the route is discovered only when it is required/needed. The process of route discovery occurs by flooding the route request packets throughout the mobile network. It consists of two major phases namely, route discovery and route maintenance.

i) Dynamic Source Routing protocol (DSR): It is a reactive/on-demand routing protocol. In this type of routing, the route is discovered only when it is required/needed. The process of route discovery occurs by flooding the route request packets throughout the mobile network. In this protocol, Source node stores the complete path information and intermediate nodes do not need to maintain routing information. It consists of two phases:
Route Discovery: This phase determines the most optimal path for the transmission of data packets between the source and the destination mobile nodes.
Route Maintenance: This phase performs the maintenance work of the route as the topology in the mobile ad-hoc network is dynamic in nature and hence, there are many cases of link breakage resulting in the network failure between the mobile nodes.

ii) Ad-Hoc On Demand Vector Routing protocol (AODV): It is a reactive/on-demand routing protocol. It is an extension of dynamic source routing protocol (DSR) and it helps to remove the disadvantage of dynamic source routing protocol. In DSR, after route discovery, when the source mobile node sends the data packet to the destination mobile node, it also contains the complete path in its header. Hence, as the network size increases, the length of

the complete path also increases and the data packet's header size also increases which makes the whole network slow.
Hence, Ad-Hoc On Demand Vector Routing protocol came as solution to it. The main difference lies in the way of storing the path, in AODV Sourcenode does not stores complete path information, instead of that each not stores information of its previous and next node. It also operates in two phases: Route discovery and Route maintenance.

iii) Hybrid Routing protocol: It basically combines the advantages of both, reactive and pro-active routing protocols. These protocols are adaptive in nature and adapts according to the zone and position of the source and destination mobile nodes. One of the most popular hybrid routing protocol is Zone Routing Protocol (ZRP).

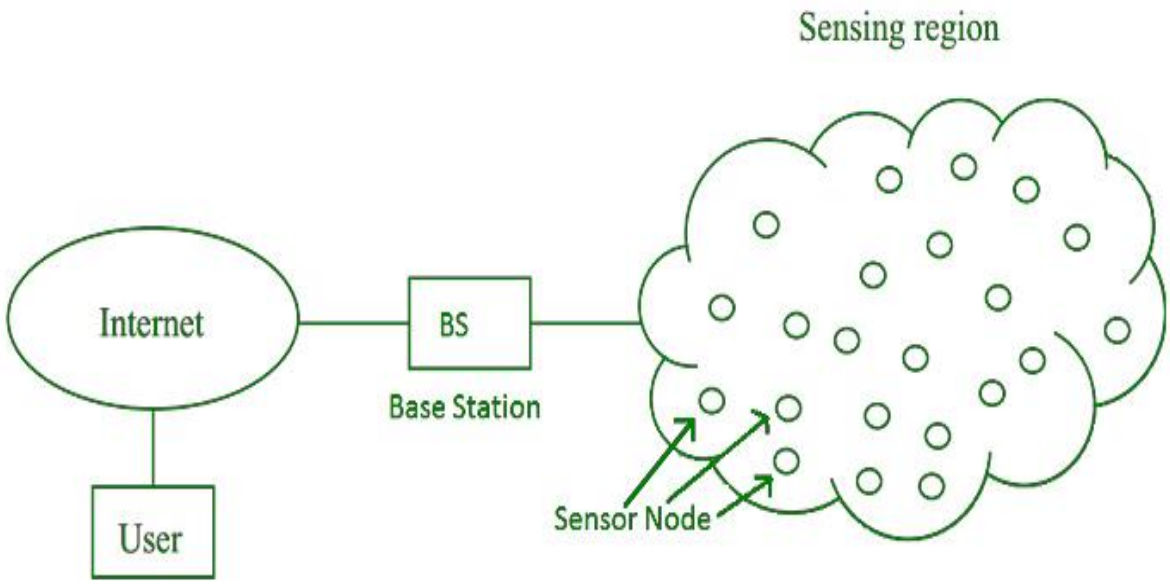
The whole network is divided into different zones and then the position of source and destination mobile node is observed. If the source and destination mobile nodes are present in the same zone, then proactive routing is used for the transmission of the data packets between them. And if the source and destination mobile nodes are present in different zones, then reactive routing is used for the transmission of the data packets between them.

Characteristics of MANET Routing Protocol:

To avoid the problems with routing in MANET, routing protocols should have following characteristics:

- It should be widely distributed.
- It must be localized.
- Because of nodes mobility, it should be adjustable to frequent change in topology.
- It must be free of impermeable routes.
- The convergence of routes must be fast.
- Each node in the network should be required to store information about the network's stable local topology.
- It should be able to provide high-quality service.

Wireless Sensor Networks: Wireless Sensor Network (WSN) is an infrastructure-less wireless network that is deployed in a large number of wireless sensors in an ad-hoc manner that is used to monitor the system, physical or environmental conditions. A Wireless Sensor Network (WSN) is a network of spatially distributed autonomous sensors that are equipped with sensors to monitor physical or environmental conditions and transmit data wirelessly to a central location for processing and analysis. These networks have gained significant importance in various applications due to their ability to provide real-time data collection, monitoring, and control in remote or harsh environments.
Sensor nodes are used in WSN with the on board processor that manages and monitors the environment in a particular area. They are connected to the Base Station which acts as a processing unit in the WSN System. Base Station in a WSN System is connected through the Internet to share data. WSN can be used for processing, analysis, storage, and mining of the data.



Sensor nodes communicate with each other and with a central base station or sink node through wireless communication. This can be achieved using various wireless protocols such as Zigbee, IEEE 802.15.4, LoRa, or Wi-Fi, depending on the application's requirements. WSNs can have different network topologies, including a star, tree, mesh, or ad-hoc network. The choice of topology depends on the specific application and requirements. Sensor nodes collect data from their environment and transmit it to a central data collection point. Data aggregation and routing techniques are often employed to minimize energy consumption and optimize data transmission. Sensor nodes are typically battery-powered and have limited energy resources. Energy-efficient protocols and techniques, such as duty cycling (where nodes periodically wake up to transmit data) and energy harvesting (generating power from the environment), are crucial for extending the network's lifespan. Sensor nodes can perform data processing, filtering, and analysis at the edge to reduce the amount of data transmitted and save energy. Advanced nodes may include more powerful processors for more complex processing tasks. WSNs must be secured to protect against data breaches and unauthorized access. Encryption and authentication mechanisms are commonly employed to ensure data confidentiality and integrity. WSNs can be highly scalable, with the ability to add or remove sensor nodes as needed. This scalability is important for accommodating changes in the monitored area or additional sensors. WSNs find applications in various fields, including environmental monitoring, precision agriculture, industrial automation, healthcare (e.g., patient monitoring), smart cities, home automation, and military applications. Designing and maintaining WSNs can be challenging due to the constraints of limited power, memory, and processing capabilities. Network resilience, routing algorithms, and interference management are some of the challenges that need to be addressed.

Wireless Sensor Networks offer a powerful means to gather real-time data from various environments, enabling improved decision-making, increased automation, and reduced costs in a wide range of industries. Their effectiveness is highly dependent on proper network design, efficient communication protocols, and careful consideration of the specific application requirements.

Components of WSN:

1. **Sensors:** Sensors in WSN are used to capture the environmental variables and which is used for data acquisition. Sensor signals are converted into electrical signals.
2. **Sensor Nodes:** Sensor nodes are the fundamental building blocks of a WSN. Each node typically includes a sensor (e.g., temperature, humidity, light, motion), a processing unit, memory, and a wireless communication module (transceiver). Sensor nodes are often battery-powered and designed for low power consumption.
3. **Radio Nodes:** It is used to receive the data produced by the Sensors and sends it to the WLAN access point. It consists of a microcontroller, transceiver, external memory, and power source.
4. **WLAN Access Point**: It receives the data which is sent by the Radio nodes wirelessly, generally through the internet.
5. **Evaluation Software:** The data received by the WLAN Access Point is processed by a software called as Evaluation Software for presenting the report to the users for further processing of the data which can be used for processing, analysis, storage, and mining of the data.

Applications of WSN:

- Internet of Things (IoT)
- Surveillance and Monitoring for security, threat detection
- Environmental temperature, humidity, and air pressure
- Noise Level of the surrounding
- Medical applications like patient monitoring
- Agriculture
- Landslide Detection

Challenges of WSN:

- Quality of Service
- Security Issue
- Energy Efficiency
- Network Throughput
- Performance
- Ability to cope with node failure
- Cross layer optimisation
- Scalability to large scale of deployment

A modern Wireless Sensor Network (WSN) faces several challenges, including:

Limited power and energy: WSNs are typically composed of battery-powered sensors that have limited energy resources. This makes it challenging to ensure that the network can function for long periods of time without the need for frequent battery replacements.
Limited processing and storage capabilities: Sensor nodes in a WSN are typically small and have limited processing and storage capabilities. This makes it difficult to perform complex tasks or store large amounts of data.

Heterogeneity: WSNs often consist of a variety of different sensor types and nodes with different capabilities. This makes it challenging to ensure that the network can function effectively and efficiently.
Security: WSNs are vulnerable to various types of attacks, such as eavesdropping, jamming, and spoofing. Ensuring the security of the network and the data it collects is a major challenge.
Scalability: WSNs often need to be able to support a large number of sensor nodes and handle large amounts of data. Ensuring that the network can scale to meet these demands is a significant challenge.
Interference: WSNs are often deployed in environments where there is a lot of interference from other wireless devices. This can make it difficult to ensure reliable communication between sensor nodes.
Reliability: WSNs are often used in critical applications, such as monitoring the environment or controlling industrial processes. Ensuring that the network is reliable and able to function correctly in all conditions is a major challenge.

Advantages of Wireless Sensor Networks (WSN):

- **Low cost:** WSNs consist of small, low-cost sensors that are easy to deploy, making them a cost-effective solution for many applications.

- **Wireless communication:** WSNs eliminate the need for wired connections, which can be costly and difficult to install. Wireless communication also enables flexible deployment and reconfiguration of the network.

- **Energy efficiency:** WSNs use low-power devices and protocols to conserve energy, enabling long-term operation without the need for frequent battery replacements.

- **Scalability:** WSNs can be scaled up or down easily by adding or removing sensors, making them suitable for a range of applications and environments.

- **Real-time monitoring:** WSNs enable real-time monitoring of physical phenomena in the environment, providing timely information for decision making and control.

Disadvantages of Wireless Sensor Networks (WSN):

- **Limited range**: The range of wireless communication in WSNs is limited, which can be a challenge for large-scale deployments or in environments with obstacles that obstruct radio signals.

- **Limited processing power**: WSNs use low-power devices, which may have limited processing power and memory, making it difficult to perform complex computations or support advanced applications.

- **Data security:** WSNs are vulnerable to security threats, such as eavesdropping, tampering, and denial of service attacks, which can compromise the confidentiality, integrity, and availability of data.

- **Interference:** Wireless communication in WSNs can be susceptible to interference from other wireless devices or radio signals, which can degrade the quality of data transmission.

- **Deployment challenges:** Deploying WSNs can be challenging due to the need for proper sensor placement, power management, and network configuration, which can require significant time and resources.

RFID Technology: Radio Frequency Identification (RFID) is a technology that uses radio waves to passively identify a tagged object. It is used in several commercial and industrial applications, from tracking items along a supply chain to keeping track of items checked out of a library.
Radio Frequency Identification (RFID) refers to a wireless system comprised of two components: tags and readers. The reader is a device that has one or more antennas that emit radio waves and receive signals back from the RFID tag. Tags, which use radio waves to communicate their identity and other information to nearby readers, can be passive or active. Passive RFID tags are powered by the reader and do not have a battery. Active RFID tags are powered by batteries.

RFID tags can store a range of information from one serial number to several pages of data. Readers can be mobile so that they can be carried by hand, or they can be mounted on a post or overhead. Reader systems can also be built into the architecture of a cabinet, room, or building.

Radio Frequency Identification is used in conjunction with a microchip, a powered antenna, and a scanner. Although commercial uses for it were first developed in the 1970s, it has become more universally accessible in recent years. With advancements to the technology used to read and store information, it is now more affordable to purchase and adapt.

Radio Frequency Identification works through a small electronic device, usually a microchip, that has information stored on it. These devices are generally quite small, sometimes the size of a grain of rice, and can hold large amounts of data. While they don't always emit electricity, some can contain a stored power source or batteries. The scanners used to read these devices can also provide enough electricity to allow them to read the microchip. There are many different uses for the technology, but it is commonly used in tracking products, animals, and currency.

Uses
RFID systems use radio waves at several different frequencies to transfer data. In health care and hospital settings, RFID technologies include the following applications:

- Inventory control
- Equipment tracking
- Out-of-bed detection and fall detection
- Personnel tracking
- Ensuring that patients receive the correct medications and medical devices
- Preventing the distribution of counterfeit drugs and medical devices
- Monitoring patients
- Providing data for electronic medical records systems

Wi-Fi Standards: Wi-Fi stands for Wireless Fidelity, and it is developed by an organization called IEEE (Institute of Electrical and Electronics Engineers) they set standards for the Wi-Fi system. Each Wi-Fi network standard has two parameters:

1. **Speed** – This is the data transfer rate of the network measured in Mbps (1 megabit per second).s
2. **Frequency** – On what radio frequency, the network is carried on. Two bands of frequency for the Wi-Fi are 2.4 GHz and 5 GHz. In short, it is the frequency of radio wave that carries data.

Two Frequencies of Wi-Fi signal: Wi-Fi routers that come with 2.4 GHz or5 GHz are called the single-band routers but a lot of new routers support both 2.4 GHz and 5 GHz frequency they are called dual-band routers.
The 2.4 GHz is a common Wi-Fi band, but it is also used by other appliances like Bluetooth devices, wireless phones, cameras, etc. Because of the signal used by so many devices, the signal becomes overcrowded and speed becomes slow. So 5 GHz comes into the picture, It is new, and not commonly used, and because it is used by fewer devices there is no signal crowding and interference.

The 2.4 GHz transmits data at a slower speed than 5 GHz but does have a longer range than 5 GHz. The 5 GHz transmits data at a faster rate, but it has a shorter range because it has a higher frequency.

Parameter	**2.4 GHz**	**5 GHz**
Speed	Comparatively Low	High
Range	High	Comparatively low

Different standards of Wi-Fi: These are the Wi-Fi standards that evolved from 1997 to 2021. In 1997 IEEE created one standard and gave the name 802.11.

IEEE 802.11 –

1. It was developed in 1997.
2. Speed is about 2 Mbps (2 megabits per second).

IEEE 802.11a –

1. This standard is developed in 1999.
2. 802.11a is useful for commercial and industrial purposes.
3. It works on a 5 GHz frequency.
4. The maximum speed of 802.11a is 54 Mbps.
5. This standard was made to avoid interference with other devices which use the 2.4 GHz band.

IEEE 802.11b –

1. This standard also created with 802.11a in 1999.
2. The difference is that it uses a 2.4 GHz frequency band.
3. The speed of 802.11b is 11 Mbps.
4. This standard is useful for home and domestic use.

IEEE 802.11g –

1. This standard is designed in 2003.
2. Basically, it has combined the properties of both 802.11a and 802.11b.
3. The frequency band used in this is 2.4 GHz for better coverage.
4. And the maximum speed is also up to 54 Mbps.

IEEE 802.11n –

1. This was introduced in 2009.
2. 802.11n operates on both 2.4 GHz and 5 GHz frequency bands, they are operated individually.
3. The data transfer rate is around 600 Mbps.

IEEE 802.11ac –

1. This standard is developed in 2013 named 802.11ac.
2. Wi-Fi 802.11ac works on the 5 GHz band.
3. The maximum speed of this standard is 1.3 Gbps.
4. It gives less range because of the 5 GHz band, but nowadays most of the devices are working on 802.11n and 802.11ac standards.

IEEE 802.11ax –

1. It is the newest and advanced version of Wi-Fi.
2. This is released in 2019.
3. Operates on both 2.4 GHz and 5 GHz for better coverage as well as better speed.
4. User will get 10 Gbps of maximum speed around 30-40 % improvement over 802.11ac

Tabular Representation:

Version	**Introduced in**	**Frequency band used**	**Maximum speed provided**
IEEE 802.11a	1999	5 GHz	54 Mbps
IEEE 802.11b	1999	2.4 GHz	11 Mbps
IEEE 802.11g	2003	2.4 GHz	54 Mbps
IEEE 802.11n	2009	Both 2.4 GHz and 5 GHz	600 Mbps
IEEE 802.11ac	2013	5 GHz	1.3 Gbps
IEEE 802.11ax	2019	Both 2.4 GHz and 5 GHz	Up to 10 Gbps

Now recently Wi-Fi alliance announced the new naming scheme for Wi-Fi standards. Rather than the complex names like "**802.11b**" name now we can call as "**Wi-Fi 1**", and similar for others. This will help consumers for easy to understand as 802.11 is difficult to understand.

New Naming Standards:

Network	Wi-Fi Standard
IEEE 802.11b	Wi-Fi 1
IEEE 802.11a	Wi-Fi 2
IEEE 802.11g	Wi-Fi 3
IEEE 802.11n	Wi-Fi 4
IEEE 802.11ac	Wi-Fi 5
IEEE 802.11ax	Wi-Fi 6

This is all about Wi-Fi and its various versions, In the future also, we may get a lot of improvements in the Wi-Fi system in speed and large range also

WiMax Standards: WiMAX technology is a wireless broadband communications technology based around the IEE 802.16 standard providing high speed data over a wide area.

The letters of WiMAX stand for Worldwide Interoperability for Microwave Access (AXess), and it is a technology for point to multipoint wireless networking.

WiMAX technology is able to meet the needs of a large variety of users from those in developed nations wanting to install a new high speed data network very cheaply without the cost and time required to install a wired network, to those in rural areas needing fast access where wired solutions may not be viable because of the distances and costs involved - effectively providing WiMAX broadband. Additionally it is being used for mobile applications, providing high speed data to users on the move.

- WiMAX aims to provide wireless broadband services with a target range of up to 31 miles at a transmission rate exceeding 100 Mbps.
- It is also to provide a wireless alternative to cable, DSL and T1/E1 for last mile access.
- The term IEEE 802.16 and WiMAX are used interchangeably.
- WiMAX is to IEEE 802.16 what Wi-Fi is to IEEE 802.11

- The acronym WiMAX stands for "Worldwide Interoperability for Microwave Access". It is based on IEEE 802.16 standard.
- IEEE 802.16 is the IEEE standard for Wireless Metropolitan Area Network (Wireless MAN).
- It specifies the air interface for fixed, portable, and mobile broadband wireless access (BWA) systems supporting multimedia services.

The IEEE 802.16, the Air Interface for Fixed Broadband Wireless Access Systems, also known as the IEEE WirelessMAN air interface, is an emerging suite of standards for fixed, portable and mobile BWA in MAN. WiMAX broadband technology uses some key technologies to enable it to provide the high speed data rates:

OFDM (Orthogonal Frequency Division Multiplex): OFDM has been incorporated into WiMAX technology to enable it to provide high speed data without the selective fading and other issues of other forms of signal format.

MIMO (Multiple Input Multiple Output): WiMAX technology makes use of multipath propagation using MIMO. By utilising the multiple signal paths that exist, the use of MIMO either enables operation with lower signal strength levels, or it allows for higher data rates.

These standards are issued by IEEE 802.16 work group that originally covered the wireless local loop (WLL) technologies in the 10.66 GHz radio spectrum, which were later extended through amendment projects to include both licensed and unlicensed spectra from 2 to 11 GHz.

The WiMAX umbrella currently includes 802.16-2004 and 802.16e. 802.16-2004 utilizes OFDM to serve multiple users in a time division fashion in a sort of a round-robin technique, but done extremely quickly so that users have the perception that they are always transmitting/receiving. 802.16e utilizes OFDMA and can serve multiple users simultaneously by allocating sets of tones to each user.

Following is the chart of various IEEE 802.16 Standards related to WiMAX.

	802.16	802.16a	802.16e
Spectrum	10 – 66 GHz	2 – 11 GHz	<6 GHz
Configuration	Line of Sight	Non- Line of Sight	Non- Line of Sight
Bit Rate	32 to 134 Mbps (28 MHz Channel)	≤ 70 or 100 Mbps (20 MHz Channel)	Up to 15 Mbps
Modulation	QPSK, 16-QAM, 64-QAM	256 Sub-Carrier OFDM using QPSK, 16-QAM, 64-QAM, 256-QAM	Same as 802.16a
Mobility	Fixed	Fixed	≤75 MPH
Channel Bandwidth	20, 25, 28 MHz	Selectable 1.25 to 20 MHz	5 MHz (Planned)
Typical Cell Radius	1-3 miles	3-5 miles	1-3 miles
Completed	Dec, 2001	Jan, 2003	2nd Half of 2005

The IEEE 802.16 standards for BWA provide the possibility for interoperability between equipment from different vendors, which is in contrast to the previous BWA industry, where proprietary products with high prices are dominant in the market.

Fem to cells Network: A Femtocell network, also known as a Femto network or Femtocell, is a type of small, low-power, and short-range cellular base station designed to enhance cellular coverage and capacity in localized areas. Femtocells are typically used in residential or small business settings to improve indoor cellular coverage, reduce network congestion, and offload traffic from the macrocellular network.
A fem to cell is a very low-range, low-power cellular base station, that can be deployed in a home, or office. It is provided by a mobile network operator and operates in licensed frequency bands. Fem to cells are used to provide network coverage to cellular devices where operator base stations or macrocells cannot reach or have weak coverage such as inside building complexes, underground structures (train stations, basement levels etc.), trains & buses etc.

Features:

- **Small Coverage Area:** Femtocells have a small coverage area, typically ranging from a few meters to a few hundred meters. They are designed to provide cellular coverage within a building or a small local area, such as a home, office, or shop.

- **Home Use:** One of the most common use cases for Femtocells is in homes. Users install the Femtocell device within their home to improve cellular reception. It connects to the user's broadband internet connection and acts as a miniature cellular base station.

- **Offloading:** Femtocells help offload cellular traffic from the macrocellular network. When a mobile device is within the coverage area of a Femtocell, it connects to the Femtocell instead of the distant macrocell, reducing congestion and improving call quality and data speeds.

- **Internet Connectivity:** Femtocells require an internet connection to backhaul voice and data traffic to the mobile operator's network. This connection can be wired (e.g., DSL, cable, fiber) or wireless (e.g., Wi-Fi or a dedicated link).

- **Security and Authentication:** Femtocells use security mechanisms to ensure that only authorized users can connect to them. This helps prevent unauthorized usage and protects the operator's network.

- **Managed by Mobile Operators:** Mobile operators typically provide and manage Femtocells for their subscribers. They control the network configuration, security, and access to the Femtocell.

- **Interference Mitigation:** Femtocell deployments require careful planning to mitigate interference with nearby macrocell networks. Various mechanisms, such as power control and frequency management, are used to minimize interference.

- **Voice and Data:** Femtocells support both voice and data services. They are compatible with various cellular standards, including 3G (UMTS/HSPA) and 4G (LTE).

- **Benefits:** The main benefits of Femtocell networks include improved indoor coverage, reduced network congestion, better call quality, and faster data speeds. They are particularly useful in areas with poor cellular coverage.

- **Challenges:** Femtocell deployments come with challenges related to network planning, interference management, and backhaul connectivity. They also require coordination with mobile operators.

The main difference between a fem to cell and a base station, microcell or picocell is the range. A base station might have a range of 20-30 km, macro cell a range of 1-2 km, picocell a range of 200-300 meters and fem to cell can have a range as low as 10 meters. However, a fem to cell uses the same licensed frequency band as the macrocell (base station). A fem to cell can coordinate with an operator base station to provide mobile devices with optimum mobile coverage by switching between fem to cells and macrocells according to signal strength. For this, the fem to cell needs to interface with the operator's base station via a fixed-line like a cable, fiber-optic or a twisted pair telephone line which is available via broadband (DSL or cable).

Fem to cells are usually separately sold or leased by a mobile network operator (MNO) to its customers. It is typically the size of a wireless router and connects to the user's broadband line. Fem to cells are plug-and-play devices and require no specific installation or technical knowledge; they can be installed by anyone at home. These devices only allow pre-declared phone numbers to connect to it which is usually done y the user through a webpage or application provided by the MNO. Fem to cells also have protection mechanisms that report changes in location to the respective MNO. Whether the MNO allows fem to cells to operate in a different location depends on the MNO's policy.

Advantages of Fem to cells

- Exceptional coverage as all connected devices are in close proximity to a fem to cell, especially in places where there is no existing signal or poor coverage.
- Fem to cells offer better voice quality (via HD voice) depending on a number of factors such as operator/network support, customer contract/price plan, phone and operating system support.
- Due to reduced transmitter-receiver distance with a fem to cell, mobile devices don't have to use as much power as when connecting to a macrocell. This improves the battery life of handsets connected to a fem to cell and also improves the overall energy efficiency of the network.
- Fem to cells may also provide higher mobile data capacity than a macrocell base station as it only serves a much smaller number of users.
- Calls placed and mobile data used under fem to cell coverage may have special tariffs depending on the pricing policy of the MNO.

Disadvantages of Fem to cells

- As Fem to cells use the same frequency bands as the conventional cellular network, they may cause interference in the wider network and also experience interference in the fem to cell network themselves. This can have a critical effect on performance and rather than improving the situation it could potentially cause problems. Hence,

fem to cells must be equipped with capable interference mitigation techniques that detect macrocells, adjust power and scramble codes accordingly.

- When using an Ethernet or ADSL connection via home broadband, the fem to cell must either share the backhaul bandwidth with other services, such as Internet browsing, gaming consoles, set-top boxes and triple-play equipment in general or alternatively directly replace these functions within an integrated unit. In shared-bandwidth scenarios, which are the majority of designs currently being developed, fem to cells may affect the quality of service for both the broadband connection and the fem to cell network.
- There is also the very likely possibility of problems arising when the provider of the broadband service differs from the mobile network provider. In such scenarios, the user may have to switch either one of their connection (broadband or mobile network) to the same company as the other.

Fem to cells were initially designed for use in wideband code division multiple access (WCDMA) networks. Later other standards like the Global System for Mobile Communications (GSM), CDMA2000, Time Division Synchronous Code Division Multiple Access (TD-SCDMA), Wi MAX, and LTE also started to support it. Many operators worldwide offer a fem to cell service, mainly targeted at businesses but also offered to individual customers (often for a one-off fee) to resolve issues regarding poor or non-existent signals at their location. Operators who have launched a fem to cell service include SFR, AT&T, C Spire, Sprint Nextel, Verizon, Zain, Mobile Tele Systems, T-Mobile US, Orange, Vodafone, EE, O2, Three etc.

Fem to cell networks are an effective solution for addressing the "dead zones" and poor indoor coverage that can be experienced with traditional macrocell networks. They help improve the overall quality of service for mobile subscribers and relieve network congestion, making them a valuable tool for mobile operators and consumers.

Push-to-talk (PTT) technology: It is a two-way communication method that allows users to have instant voice conversations by pressing a button or activating a virtual switch. It is commonly associated with walkie-talkie devices and radio communication systems. While PTT is primarily used for voice communication, there isn't a direct equivalent for SMS (text messaging) as PTT is designed for real-time voice communication.

Features:

- **Instant Messaging Apps:** Many instant messaging apps offer a "voice message" feature, which allows users to record a short voice message and send it to their contacts. Although this is not SMS, it provides a quick and convenient way to send voice snippets instead of text.

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

- **Group Chats**: Group chat features in messaging apps can be somewhat akin to a PTT group conversation. Multiple users can participate in a single chat, and messages are sent in real-time.

- **Enterprise Solutions**: In a business or enterprise context, there are communication and collaboration tools that offer text messaging, voice messaging, and even video conferencing, providing a broader range of communication options.

While these features don't replicate the exact PTT experience of real-time voice communication, they offer a way to communicate quickly with voice or text, and they can be very useful for various scenarios. The choice of communication method depends on the specific needs and preferences of users and the context in which they are communicating.