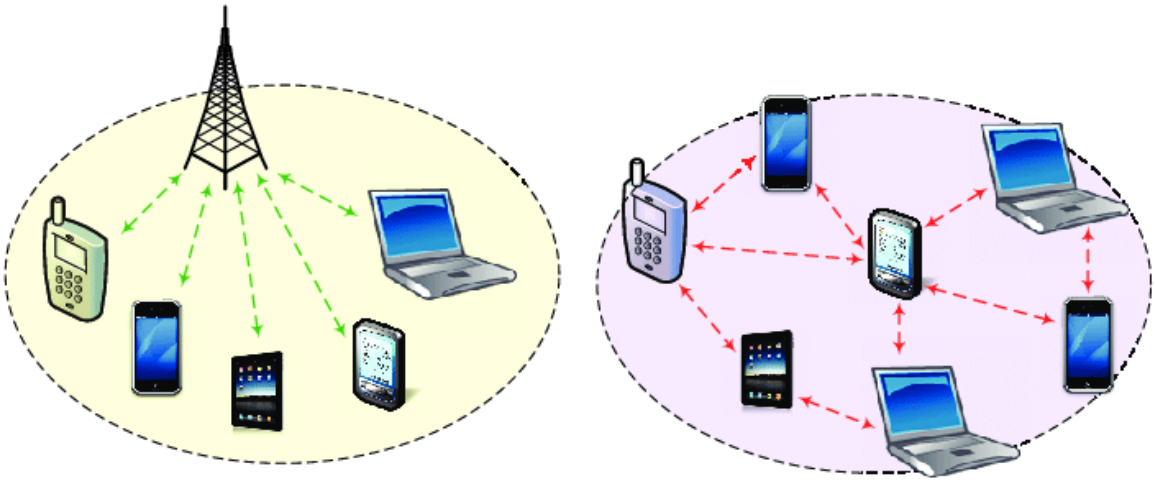
Unit-3

*Difference between Radio wave and Infrared waves:

Sr. No.	Basis	Radiowave	Infrared wave
1.	Direction	These are omni-directional in nature.	These are unidirectional in nature.
2.	Penetration	At low frequency, they can penetrate through solid objects and walls but high frequency they bounce off the obstacle.	They cannot penetrate through any solid object and walls.
3.	Frequency range	Frequency range: 3 KHz to 1GHz.	Frequency range: 300 GHz to 400 GHz.
4.	Security	These offers poor security.	These offers high security.
5.	Attenuation	Attenuation is high.	Attenuation is low.
6.	Government License	Some frequencies in the radio-waves require government license to use these.	There is no need of government license to use these waves.
7.	Usage Cost	Setup and usage Cost is moderate.	Usage Cost is very less.
8.	Communication	These are used in long distance communication.	These are not used in long distance communication.

*Infrastructure and Ad-hoc Networks:



Infrastructure-based wireless networks

Wireless ad hoc networks

Infrastructure mode is when the wireless network requires a physical structure to support it. This essentially means there should be a medium handling the network functions, creating an infrastructure around which the network sustains.

It performs these typical **functions**:

- Providing access to other networks
- Forwarding
- Medium access control

In infrastructure-based wireless networks, the communication takes place between the wireless nodes (i.e., endpoints in the network such as your computer, your phone, etc.) and the access points (i.e., the router) only.

There can be more than one access point on the same network handling different wireless nodes.

A typical example of an infrastructure network would be cellular phone networks. They have to have a set infrastructure (i.e., network towers) to function.

Advantages:

- Infrastructure network provides a centralized management system.
- Infrastructure network can cover a larger area.
- Higher bandwidth.

Disadvantages:

- High Infrastructure cost.
- Limited mobility.
- Infrastructure network is vulnerable to security risks.

Ad-hoc wireless networks, on the other hand, do not require a set infrastructure to work. In ad-hoc networks, each node can communicate with other nodes, so no access point that provides access control is required.

Whereas the routing in infrastructure networks is taken care of by the access point, in ad-hoc networks the nodes in the network take care of **routing**.

Routing is to find the best possible path between the source and destination nodes to transfer data.

All the individual nodes in an ad-hoc network maintain a routing table, which contains the information about the other nodes. As the nature of the ad-hoc network is dynamic, this results in ever-changing router tables. One important thing to note is that an ad-hoc network is asymmetric by nature, meaning the path of data upload and download between two nodes in the network may be different.

A typical example of an ad-hoc network is connecting two or more laptops (or other supported devices) to each other directly without any central access point, either wirelessly or using a cable.

Advantages:

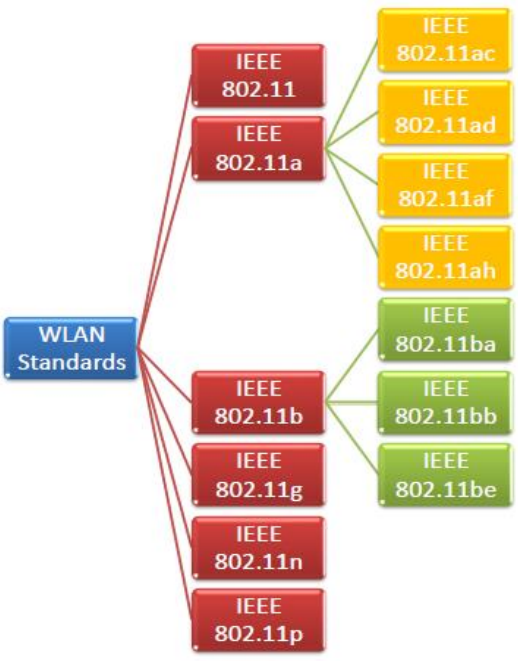
- Ad hoc networks are highly flexible.
- Ad hoc networks are cost-effective.
- It is decentralized.

Disadvantages:

- Network Instability.
- Ad hoc networks typically have a limited range.
- Ad hoc networks are more vulnerable to security threats.

*** IEEE 802.11WLAN Standards:**

The IEEE 802.11 WLAN Standards are a set of specifications developed by the Institute of Electrical and Electronics Engineers (IEEE) for wireless local area networks (WLANs). These standards define the protocols and technologies used to establish wireless network connections, including data transfer rates, frequency bands, and security measures.



There are several standards of IEEE 802.11 WLANs. The prominent among them are 802.11, 802.11a, 802.11b, 802.11g, 802.11n and 802.11p. All the standards use carrier-sense multiple access with collision avoidance (CSMA/CA). Also, they have support for both centralised base station based as well as ad hoc networks.

IEEE 802.11:

It provided 1 Mbps or 2 Mbps data rate in the 2.4 GHz band and used either frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS). It is obsolete now.

IEEE 802.11a:

It provides a maximum data rate of 54 Mbps operating in the 5 GHz band. Besides it provides error correcting code. As 2.4 GHz band is crowded, relatively sparsely used 5 GHz imparts additional advantage to 802.11a.

Further amendments to 802.11a are 802.11ac, 802.11ad, 802.11af, 802.11ah, 802.11ai, 802.11aj etc.

IEEE 802.11b:

It has a higher data rate of 11 Mbps operates in the 2.4 GHz band. However, since 2.4 GHz band is pretty crowded, 802.11b devices faces interference from other devices.

Further amendments to 802.11b are 802.11ba, 802.11bb, 802.11bc, 802.11bd and 802.11be.

IEEE 802.11g:

It operates in the 2.4 GHz band (as in 802.11b) and provides a average throughput of 22 Mbps. It uses OFDM technique (as in 802.11a). It is fully backward compatible with 802.11b. 802.11g devices also faces interference from other devices operating in 2.4 GHz band.

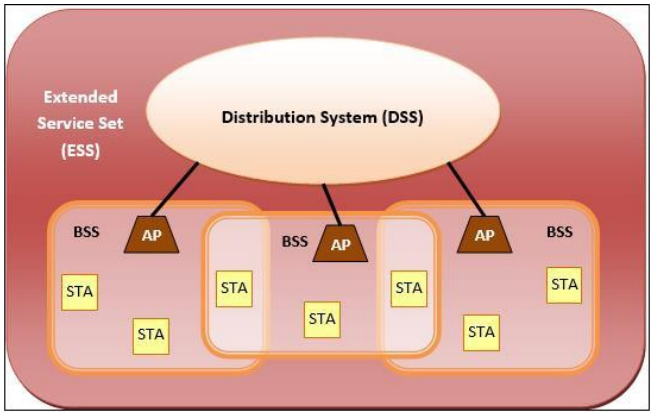
IEEE 802.11n:

802.11n operates on both the 2.4 GHz and the 5 GHz bands. It has variable data rate ranging from 54 Mbps to 600 Mbps. It provides a marked improvement over previous standards 802.11 by incorporating multiple-input multiple-output antennas (MIMO antennas).

IEEE 802.11p:

802.11 is an amendment for including wireless access in vehicular environments (WAVE) to support Intelligent Transportation Systems (ITS). They include network communications between vehicles moving at high speed and the environment. They have a data rate of 27 Mbps and operate in 5.9 GHz band.

*Architecture of wireless LAN:



Wireless LANs are those Local Area Networks that use 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. Most WLANs are based upon the standard IEEE 802.11 or WiFi.

IEEE 802.11 Architecture

The components of an IEEE 802.11 architecture are as follows

1) Stations (STA) − Stations comprise all devices and equipments that are connected to the wireless LAN. A station can be of two types:

Wireless Access Pointz (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.

2) Basic Service Set (BSS) −A basic service set is a group of stations communicating at physical layer level. BSS can be of two categories depending upon mode of operation:

Infrastructure BSS − Here, the devices communicate with other devices through access points.

Independent BSS − Here, the devices communicate in peer-to-peer basis in an ad hoc manner.

3) Extended Service Set (ESS) − It is a set of all connected BSS.

4) Distribution System (DS) − It connects access points in ESS.

Advantages of WLANs

- They provide clutter free homes, offices and other networked places.
- The LANs are scalable in nature, i.e. devices may be added or removed from the network at a greater ease than wired LANs.
- The system is portable within the network coverage and access to the network is not bounded by the length of the cables.
- Installation and setup is much easier than wired counterparts.
- The equipment and setup costs are reduced.

Disadvantages of WLANs

- Since radio waves are used for communications, the signals are noisier with more interference from nearby systems.
- Greater care is needed for encrypting information. Also, they are more prone to errors. So, they require greater bandwidth than the wired LANs.
- WLANs are slower than wired LANs.

*Wireless Lan services:

Wireless LAN (WLAN) services refer to the various services provided by wireless networks, such as Wi-Fi, that allow wireless communication between devices over a local area network. Here are some common wireless LAN services:

- **Internet access**: WLAN services provide wireless internet access, allowing devices to connect to the internet without the need for a physical connection to a router or modem. This service is commonly available in public places, such as airports, coffee shops, and hotels, as well as in homes and offices.

- **File sharing**: WLAN services allow devices to share files wirelessly, making it easier to transfer files between devices without the need for physical media or cables.
- **Streaming media:** WLAN services allow devices to stream media, such as video or music, over the wireless network. This service is commonly used for streaming services like Netflix and Spotify.
- **Voice over IP (VoIP):** WLAN services can be used to provide voice over IP (VoIP) services, which allow users to make voice calls over the internet using their devices. This service is commonly used in business environments for conference calling and remote meetings.
- **Remote access:** WLAN services can be used to provide remote access to devices on the network, allowing users to access files and applications from a remote location. This service is commonly used by businesses for remote workers.
- **Location-based services:** WLAN services can be used to provide location-based services, such as indoor navigation or asset tracking, by using wireless access points to determine the location of devices on the network.

*Hiper Lan:

HIPERLAN (High-Performance Radio Local Area Network) is a wireless communication technology developed by the European Telecommunications Standards Institute (ETSI). HIPERLAN was designed as a European alternative to the American-developed IEEE 802.11 Wi-Fi standard. It operates in the 5 GHz frequency band and supports data transfer rates of up to 54 Mbps, which was considered high-speed at the time of its development.

It supports a packet-oriented structure, which can be used for networks with or without a central control (BS-MS and ad-hoc). It supports 25 audio connections at 32kbps with a maximum latency of 10 ms, one video connection of 2 Mbps with 100 ms latency, and a data rate of 13.4 Mbps.

The goals of HiperLAN are as follows:

Strong security

Handoff when moving between local area and wide areas

Increased throughput

Ease of use, deployment, and maintenance

Affordability

Scalability

**There are two types of HIPERLAN, HIPERLAN/1 and HIPERLAN/2, each with its own features and capabilities.

HIPERLAN/1:

- Operates in the 5 GHz frequency band
- Supports data transfer rates of up to 23.5 Mbps
- Uses frequency-hopping spread spectrum (FHSS) technology
- Supports up to 32 simultaneous connections
- Provides support for quality of service (QoS) and security mechanisms, such as encryption and authentication protocols

HIPERLAN/2:

- Operates in the 5 GHz frequency band

- Supports data transfer rates of up to 54 Mbps
- Uses direct sequence spread spectrum (DSSS) technology
- Supports up to 64 simultaneous connections
- Provides support for quality of service (QoS) and security mechanisms, such as encryption and authentication protocols
- Supports packet-based and connection-oriented services
- Provides support for real-time applications, such as voice and video
- Supports roaming between access points without interruption of service

*Bluetooth:

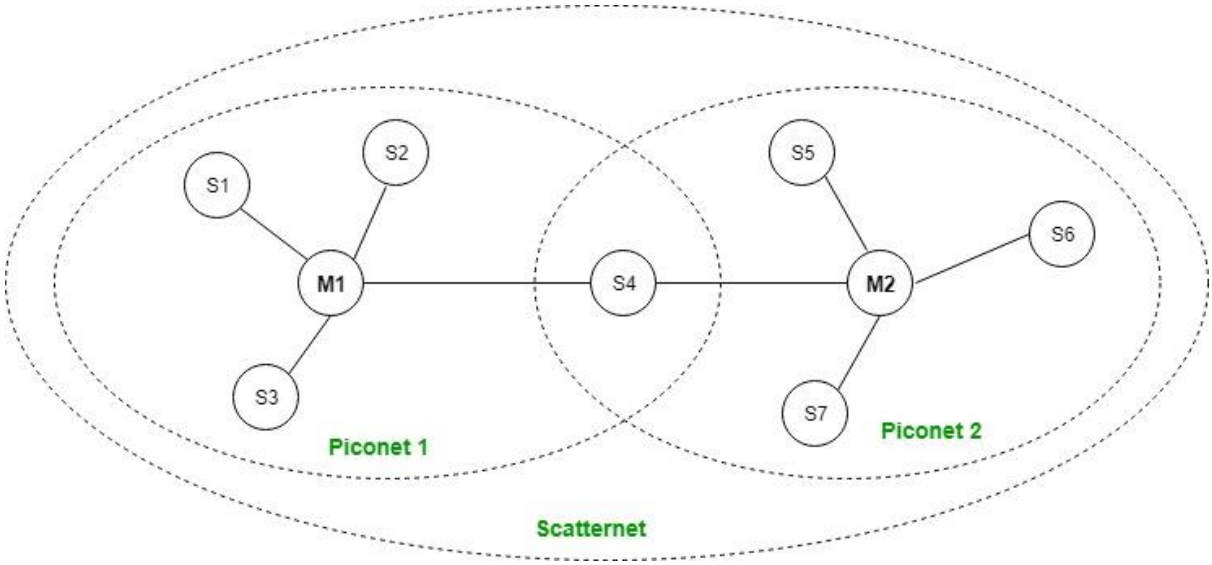
Bluetooth simply follows the principle of transmitting and receiving data using radio waves. It can be paired with the other device which has also Bluetooth but it should be within the estimated communication range to connect. When two devices start to share data, they form a network called piconet which can further accommodate more than five devices.

Bluetooth Architecture:

The architecture of Bluetooth defines two types of networks:

1. Piconet

2. Scatternet



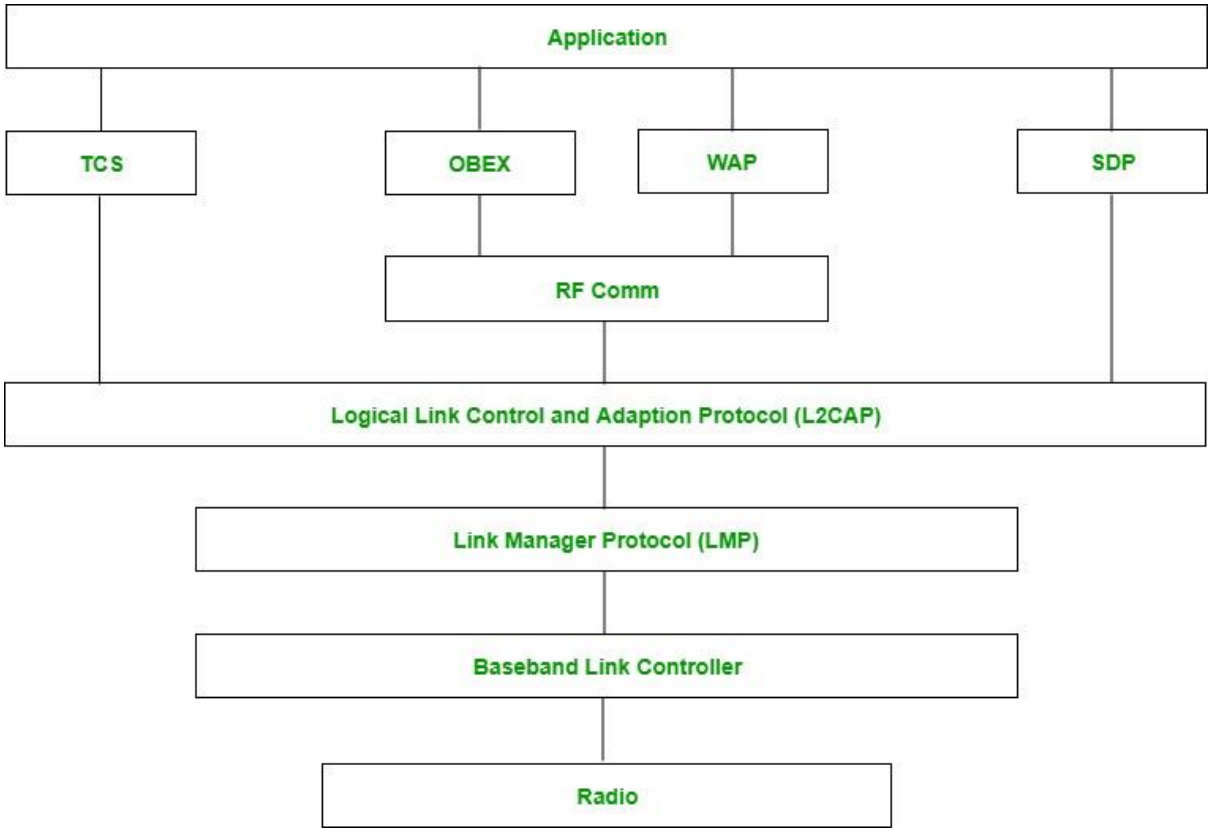
Piconet:

Piconet is a type of Bluetooth network that contains one primary node called the master node and seven active secondary nodes called slave nodes. Thus, we can say that there is a total of 8 active nodes which are present at a distance of 10 meters. The communication between the primary and secondary nodes can be one-to-one or one-to-many. Possible communication is only between the master and slave; Slave-slave communication is not possible. It also has 255 parked nodes, these are secondary nodes and cannot take participation in communication unless it gets converted to the active state.

Scatternet:

It is formed by using various piconets. A slave that is present in one piconet can act as master or we can say primary in another piconet. This kind of node can receive a message from a master in one piconet and deliver the message to its slave in the other piconet where it is acting as a master. This type of node is referred to as a bridge node. A station cannot be mastered in two piconets.

Bluetooth protocol stack:



1)Radio (RF) layer: It specifies the details of the air interface, including frequency, the use of frequency hopping and transmit power. It performs modulation/demodulation of the data into RF signals. It defines the physical characteristics of Bluetooth transceivers. It defines two types of physical links: connection-less and connection-oriented.

2)Baseband Link layer: The baseband is the digital engine of a Bluetooth system and is equivalent to the MAC sublayer in LANs. It performs the connection establishment within a piconet, addressing, packet format, timing and power control.

3)Link Manager protocol layer: It performs the management of the already established links which includes authentication and encryption processes. It is responsible for creating the links, monitoring their health, and terminating them gracefully upon command or failure.

4)Logical Link Control and Adaption (L2CAP) Protocol layer: It is also known as the heart of the Bluetooth protocol stack. It allows the communication between upper and lower layers of the Bluetooth protocol stack. It packages the data packets received from upper layers into the form expected by lower layers. It also performs segmentation and multiplexing.

5)Service Discovery Protocol (SDP) layer: It is short for Service Discovery Protocol. It allows discovering the services available on another Bluetooth-enabled device.

6)RF comm layer: It is a cabal replacement protocol. It is short for Radio Frontend Component. It provides a serial interface with WAP and OBEX. It also provides emulation of serial ports over the logical link control and adaption protocol(L2CAP). The protocol is based on the ETSI standard TS 07.10.

7)OBEX: It is short for Object Exchange. It is a communication protocol to exchange objects between 2 devices.

8)WAP: It is short for Wireless Access Protocol. It is used for internet access.

9)TCS: It is short for Telephony Control Protocol. It provides telephony service. The basic function of this layer is call control (setup & release) and group management for the gateway serving multiple devices.

10)Application layer: It enables the user to interact with the application.