# LECTURE NOTES

# ON

# WIRELESS LANS AND PANS

**M.Tech I semester**
**(Autonomous-IARE-R18)**

**Prepared by**

**Mr. C.DEVISUPRAJA, Asst. Professor**


**ELECTRONICS AND COMMUNICATION ENGINEERING**

**INSTITUTE OF AERONAUTICAL ENGINEERING**
**(Autonomous)**
**Dundigal, Hyderbad-500043**

# UNIT-1

# WIRELESS SYSTEM&RANDOM ACCESS PROTOCOLS

In the most general sense, a wireless system is any collection of elements (or subsystems) that operate interdependently and use unguided electromagnetic-wave propagation to perform some specified function(s). Some examples of systems that fit this definition are

- Systems that convey information between two or more locations, such as personal communication systems (PCS), police and fire department radio systems, commercial broadcast systems, satellite broadcast systems, telemetry and remote monitoring systems.
- Systems that sense the environment and/or objects in the environment, including radar systems that may be used for detecting the presence of objects in some region or volume of the environment and measuring their relative motion and/or position, systems for sensing or measuring atmospheric conditions, and systems for mapping the surface of the Earth or planets.
- Systems that aid in navigation or determine the location of an object on the Earth or in space.

## First and Second Generation Cellular Systems

### 1G: Analog Cellular Networks

The main technological development that distinguished the First Generation mobile phones from the previous generation was the use of multiple cell sites, and the ability to transfer calls from one site to the next as the user travelled between cells during a conversation. The first commercially automated cellular network (the 1G generations) was launched in Japan by NTT in 1979.

In 1984, Bell Labs developed modern commercial cellular technology, which employed multiple, centrally controlled base stations (cell sites), each providing service to a small area (a cell). The cell sites would be set up such that cells partially overlapped. In a cellular system, a signal between a base station (cell site) and a terminal (phone) only need be strong enough to reach between the two, so the same channel can be used simultaneously for separate conversations in different cells.

As the system expanded and neared capacity, the ability to reduce transmission power allowed new cells to be added, resulting in more, smaller cells and thus more capacity.

**2G: Digital Networks**

In the 1990s, the 'second generation' (2G) mobile phone systems emerged, primarily using theGSM standard. These 2G phone systems differed from the previous generation in their use of digital transmission instead of analog transmission, and also by the introduction of advanced and fast phone-to-network signaling. The rise in mobile phone usage as a result of 2G was explosive and this era also saw the advent of prepaid mobile phones.

The second generation introduced a new variant to communication, as SMS text messaging became possible, initially on GSM networks and eventually on all digital networks. Soon SMS became the communication method of preference for the youth. Today in many advanced markets the general public prefers sending text messages to placing voice calls.

Some benefits of 2G were Digital signals require consume less battery power, so it helps mobile batteries to last long. Digital coding improves the voice clarity and reduces noise in the line. Digital signals are considered environment friendly. Digital encryption has provided secrecy and safety to the data and voice calls. The use of 2G technology requires strong digital signals to help mobile phones work properly.

**“2.5G” using GPRS (General Packet Radio Service)** technology is a cellular wireless technology developed in between its predecessor, 2G, and its successor, 3G. GPRS could provide data rates from 56 kbit/s up to 115 kbit/s. It can be used for services such as Wireless Application Protocol (WAP) access, Multimedia Messaging Service (MMS), and for Internet communication services such as email and World Wide Web access.

**2.75 – EDGE** is an abbreviation for Enhanced Data rates for GSM Evolution. EDGE technology is an extended version of GSM. It allows the clear and fast transmission of data and information up to 384kbit/s speed.

**4G: Growth of mobile broadband**

Consequently, the industry began looking to data-optimized 4th-generation technologies, with the promise of speed improvements up to 10-fold over existing 3G technologies. It is basically the extension in the 3G technology with more bandwidth and services offers in the 3G. The expectation for the 4G technology is basically the high quality audio/video streaming

over end to end Internet Protocol.The first two commercially available technologies billed as 4G were the WiMAX standard and the LTE standard, first offered in Scandinavia by TeliaSonera.

One of the main ways in which 4G differed technologically from 3G was in its elimination of circuit switching, instead employing an all-IP network. Thus, 4G ushered in a treatment of voice calls just like any other type of streaming audio media, utilizing packet switching overinternet, LAN or WAN networks via VoIP.

4G LTE data transfer speed can reach peak download 100 Mbit/s, peak upload 50 Mbit/s, WiMAX offers peak data rates of 128 Mbit/s downlink and 56 Mbit/s uplink.

**The following are some possible features of the 4G systems :**

1. Support interactive multimedia, voice, video, wireless internet and other broadband services.
2. High speed, high capacity and low cost per bit.
3. Global mobility, service portability, scalable mobile networks.
4. Seamless switching, variety of services based on Quality of Service (QoS) requirements
5. Better scheduling and call admission control techniques.
6. Ad hoc networks and multi-hop networks.

**The Wireless Spectrum**

The wireless spectrum consists of electromagnetic radiation and frequency bands. Respective countries have their own wireless spectra with ranges up to 300 GHz. The wireless spectrum frequencies used in communication are regulated by national organizations, which specify which frequency ranges can be used by whom and for which purpose.

Radio-channel and channel-frequency variation is quite complex because radio propagation characteristics are a result of both man-made and natural factors. Government entities own frequency channels, which are divided according to common frequency band characteristics and cause performance breaks at different frequency levels, where only windows of continuity are available.

**A PURE ALOHA**

A protocol for satellite and terrestrial radio transmissions. In pure Aloha, a user can transmit at any time but risks collisions with other users' messages. "Slotted Aloha" reduces the

chance of collisions by dividing the channel into time slots and requiring that the user send only at the beginning of a time slot. Aloha was the basis for Ethernet, a local area network protocol.

- It allows the stations to transmit data at any time whenever they want.
- After transmitting the data packet, station waits for some time.

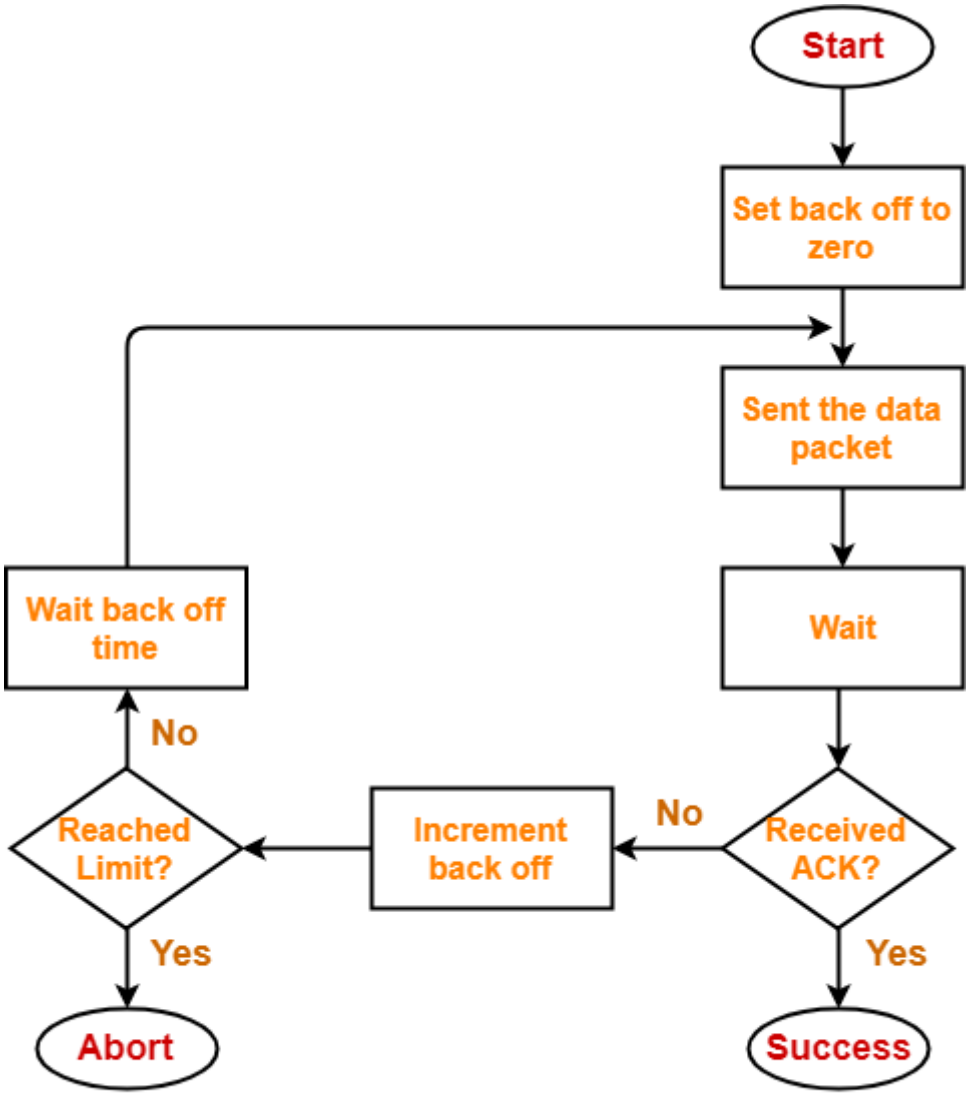
**Then, following 2 cases are possible-**

**Case-01:**

- Transmitting station receives an acknowledgement from the receiving station.
- In this case, transmitting station assumes that the transmission is successful.

**Case-02:**

- Transmitting station does not receive any acknowledgement within specified time from the receiving station
- In this case, transmitting station assumes that the transmission is unsuccessful.
- Transmitting station uses a **Back Off Strategy** and waits for some random amount of time.
- After back off time, it transmits the data packet againIt keeps trying until the back off limit is reached after which it aborts the transmission.




Flowchart for Pure Aloha

**Efficiency-**

Efficiency of Pure Aloha ($\eta$) = G x $e^{-2G}$

where G = Number of stations willing to transmit data

**Maximum Efficiency-**

For maximum efficiency,

- We put $d\eta / dG = 0$

- Maximum value of η occurs at G = 1/2
- Substituting G = 1/2 in the above expression, we get-

Maximum efficiency of Pure Aloha

$= 1/2 \times e^{-2 \times 1/2}$

$= 1 / 2e$

$= 0.184$

$= 18.4\%$

Thus,

| Maximum Efficiency of Pure Aloha (η) = 18.4% |
|---|

The maximum efficiency of Pure Aloha is very less due to large number of collisions.

**2. Slotted Aloha-**

- Slotted Aloha divides the time of shared channel into discrete intervals called as **time slots**.
- Any station can transmit its data in any time slot.
- The only condition is that station must start its transmission from the beginning of the time slot.
- If the beginning of the slot is missed, then station has to wait until the beginning of the next time slot.
- A collision may occur if two or more stations try to transmit data at the beginning of the same time slot.

**Efficiency-**

| Efficiency of Slotted Aloha (η) = $G \times e^{-G}$ |
|---|

where G = Number of stations willing to transmit data at the beginning of the same time slot

**Maximum Efficiency-**

For maximum efficiency,

- We put $d\eta / dG = 0$
- Maximum value of $\eta$ occurs at $G = 1$
- Substituting $G = 1$ in the above expression, we get-

Maximum efficiency of Slotted Aloha

$= 1 \times e^{-1}$

$= 1 / e$

$= 0.368$

$= 36.8\%$

Thus,

| Maximum Efficiency of Slotted Aloha ($\eta$) = 36.8% |
|---|

The maximum efficiency of Slotted Aloha is high due to less number of collisions.

Carrier-sense multiple access

**Carrier-sense multiple access** (**CSMA**) is a media access control (MAC) protocol in which a node verifies the absence of other traffic before transmitting on a shared transmission medium, such as an electrical bus or a band of the electromagnetic spectrum.

A transmitter attempts to determine whether another transmission is in progress before initiating a transmission using a carrier-sense mechanism. That is, it tries to detect the presence of a carrier signal from another node before attempting to transmit. If a carrier is sensed, the node waits for the transmission in progress to end before initiating its own transmission. Using CSMA, multiple nodes may, in turn, send and receive on the same medium. Transmissions by one node are generally received by all other nodes connected to the medium.

Variations on basic CSMA include addition of collision-avoidance, collision-detection and collision-resolution techniques.

Access modes

Variations of CSMA use different algorithms to determine when to initiate transmission onto the shared medium. A key distinguishing feature of these algorithms is how aggressive or persistent they are in initiating transmission. A more aggressive algorithm may begin

transmission more quickly and utilize a greater percentage of available bandwidth of the medium. This is typically at the expense of increased likelihood of collision with other transmitters.

**1-persistent**

1-persistent CSMA is an aggressive transmission algorithm. When the transmitting node is ready to transmit, it senses the transmission medium for idle or busy. If idle, then it transmits immediately. If busy, then it senses the transmission medium continuously until it becomes idle, then transmits the message (a frame) unconditionally (i.e. with probability=1). In case of a collision, the sender waits for a random period of time and attempts the same procedure again. 1-persistent CSMA is used in CSMA/CD systems including Ethernet.

**Non-persistent**

Non persistent CSMA is a non aggressive transmission algorithm. When the transmitting node is ready to transmit data, it senses the transmission medium for idle or busy. If idle, then it transmits immediately. If busy, then it waits for a random period of time (during which it does not sense the transmission medium) before repeating the whole logic cycle (which started with sensing the transmission medium for idle or busy) again. This approach reduces collision, results in overall higher medium throughput but with a penalty of longer initial delay compared to 1–persistent.

**P-persistent**

This is an approach between 1-persistent and non-persistent CSMA access modes.[1] When the transmitting node is ready to transmit data, it senses the transmission medium for idle or busy. If idle, then it transmits immediately. If busy, then it senses the transmission medium continuously until it becomes idle, then transmits with probability *p*. If the node does not transmit (the probability of this event is *1-p*), it waits until the next available time slot. If the transmission medium is not busy, it transmits again with the same probability *p*. This probabilistic hold-off repeats until the frame is finally transmitted or when the medium is found to become busy again (i.e. some other node has already started transmitting). In the latter case the node repeats the whole logic cycle (which started with sensing the transmission medium for idle or busy) again. p-persistent CSMA is used in CSMA/CA systems including Wi-Fi and other packet radio systems.

**O-persistent**

Each node is assigned a transmission order by a supervisory node. When the transmission medium goes idle, nodes wait for their time slot in accordance with their assigned transmission order. The node assigned to transmit first transmits immediately. The node

assigned to transmit second waits one time slot (but by that time the first node has already started transmitting). Nodes monitor the medium for transmissions from other nodes and update their assigned order with each detected transmission (i.e. they move one position closer to the front of the queue). O-persistent CSMA is used by CobraNet, LonWorks and the controller area network.

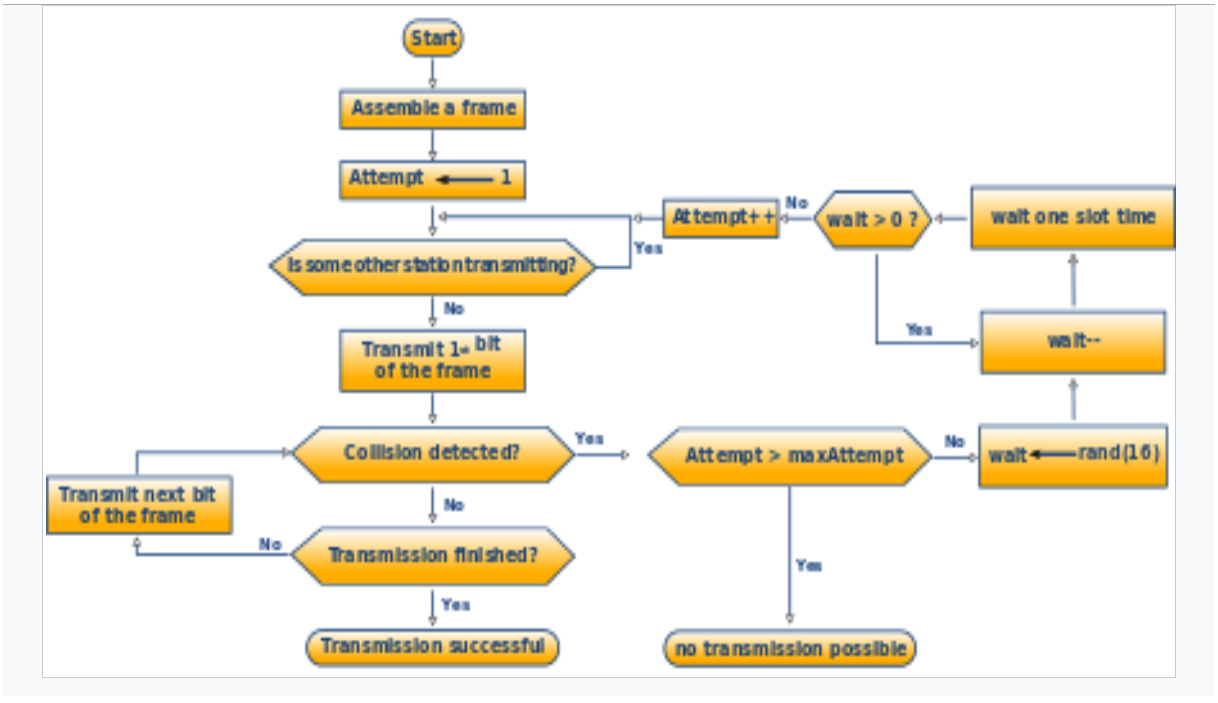
**Carrier Sense Multiple Access with Collision Detection (CSMA/CD)**

Carrier-sense multiple access with collision detection (CSMA/CD) is a media access control method used most notably in early Ethernet technology for local area networking. It uses carrier-sensing to defer transmissions until no other stations are transmitting. This is used in combination with collision detection in which a transmitting station detects collisions by sensing transmissions from other stations while it is transmitting a frame. When this collision condition is detected, the station stops transmitting that frame, transmits a jam signal, and then waits for a random time interval before trying to resend the frame.

CSMA/CD is a modification of pure carrier-sense multiple access (CSMA). CSMA/CD is used to improve CSMA performance by terminating transmission as soon as a collision is detected, thus shortening the time required before a retry can be attempted.

With the growing popularity of Ethernet switches in the 1990s, IEEE 802.3 deprecated Ethernet repeaters, CSMA/CD, and half-duplex operation in 2011, rendering CSMA/CD largely obsolete.

**Procedure**



Simplified algorithm of CSMA/CD including retransmission logic used to resolve a detected collision.

The following procedure is used to initiate a transmission. The procedure is complete when the frame is transmitted successfully or a collision is detected during transmission.

1. Is a frame ready for transmission? If not, wait for a frame.
2. Is medium idle? If not, wait until it becomes ready.
3. Start transmitting and monitor for collision during transmission.
4. Did a collision occur? If so, go to collision detected procedure.
5. Reset retransmission counters and complete frame transmission.

The following procedure is used to resolve a detected collision. The procedure is complete when retransmission is initiated or the retransmission is aborted due to numerous collisions.

1. Continue transmission (with a jam signal instead of frame header/data/CRC) until minimum packet time is reached to ensure that all receivers detect the collision.
2. Increment retransmission counter.
3. Was the maximum number of transmission attempts reached? If so, abort transmission.
4. Calculate and wait the random backoff period based on number of collisions.
5. Re-enter main procedure at stage 1.

Methods for collision detection are media dependent. On a shared, electrical bus such as 10BASE5 or 10BASE2, collisions can be detected by comparing transmitted data with received data or by recognizing a higher than normal signal amplitude on the bus. On all other media, a carrier sensed on the receive channel while transmitting triggers a collision event. Repeaters or hubs detect collisions on their own and propagate jam signals.

The collision recovery procedure can be likened to what happens at a dinner party, where all the guests talk to each other through a common medium (the air). Before speaking, each guest politely waits for the current speaker to finish. If two guests start speaking at the same time, both stop and wait for short, random periods of time (in Ethernet, this time is measured in microseconds). The hope is that by each choosing a random period of time, both guests will not choose the same time to try to speak again, thus avoiding another collision.

**Applications**

CSMA/CD was used in now-obsolete shared media Ethernet variants (10BASE5, 10BASE2) and in the early versions of twisted-pair Ethernet which used repeater hubs. Modern Ethernet networks, built with switches and full-duplex connections, no longer need to use CSMA/CD because each Ethernet segment, or collision domain, is now isolated. CSMA/CD is still

supported for backwards compatibility and for half-duplex connections. The IEEE 802.3 standard, which defines all Ethernet variants, for historical reasons still bore the title "Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications" until 802.3-2008, which uses new name "IEEE Standard for Ethernet".

**Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).**

Carrier-sense multiple access with collision avoidance (CSMA/CA) in computer networking, is a network multiple access method in which carrier sensing is used, but nodes attempt to avoid collisions by beginning transmission only after the channel is sensed to be "idle". When they do transmit, nodes transmit their packet data in its entirety.

It is particularly important for wireless networks, where the collision detection of the alternative CSMA/CD is not possible due to wireless transmitters desensing their receivers during packet transmission.

CSMA/CA is unreliable due to the hidden node problem.

CSMA/CA is a protocol that operates in the Data Link Layer (Layer 2) of the OSI model**.**

**Details**

Collision avoidance is used to improve the performance of the CSMA method by attempting to divide the channel somewhat equally among all transmitting nodes within the collision domain.

1. **Carrier Sense**: prior to transmitting, a node first listens to the shared medium (such as listening for wireless signals in a wireless network) to determine whether another node is transmitting or not. Note that the hidden node problem means another node may be transmitting which goes undetected at this stage.
2. **Collision Avoidance**: if another node was heard, we wait for a period of time (usually random) for the node to stop transmitting before listening again for a free communications channel.

- **Request to Send/Clear to Send** (RTS/CTS) may optionally be used at this point to mediate access to the shared medium. This goes some way to alleviating the problem of hidden nodes because, for instance, in a wireless network, the Access Point only issues a *Clear to Send* to one node at a time. However, wireless 802.11 implementations do not typically implement RTS/CTS for all transmissions; they may turn it off completely, or at least not use it for small packets (the overhead of RTS, CTS and transmission is too great for small data transfers).

- **Transmission**: if the medium was identified as being clear *or* the node received a CTS to explicitly indicate it can send, it sends the frame in its entirety. Unlike CSMA/CD, it is very challenging for a wireless node to listen at the same time as it transmits (its transmission will dwarf any attempt to listen). Continuing the wireless example, the node awaits receipt of an acknowledgement packet from the Access Point to indicate the packet was received and check summed correctly. If such acknowledgement does not arrive in a timely manner, it assumes the packet collided with some other transmission, causing the node to enter a period of binary exponential backoff prior to attempting to re-transmit.

  Although CSMA/CA has been used in a variety of wired communication systems, it is particularly beneficial in a wireless LAN due to a common problem of multiple stations being able to see the Access Point, but not each other. This is due to differences in transmit power, and receive sensitivity, as well as distance, and location with respect to the AP. This will cause a station to not be able to 'hear' another station's broadcast. This is the so-called 'hidden node', or 'hidden station' problem. Devices utilizing 802.11 based standards can enjoy the benefits of collision avoidance (RTS / CTS handshake, also Point coordination function), although they do not do so by default. By default they use a Carrier sensing mechanism called 'exponential backoff', or (Distributed coordination function) that relies upon a station attempting to 'listen' for another station's broadcast before sending. CA, or PCF relies upon the AP (or the 'receiver' for Ad hoc networks) granting a station the exclusive right to transmit for a given period of time after requesting it (Request to Send / Clear to Send).

# UNIT-II

# WIRELESS LANS

A wireless LAN (WLAN) is a wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area such as a home, school, computer laboratory, campus, office building etc. This gives users the ability to move around within the area and yet still be connected to the network. Through a gateway, a WLAN can also provide a connection to the wider Internet.Most modern WLANs are based on IEEE 802.11 standards and are marketed under the Wi-Fi brand name.

Wireless LANs have become popular for use in the home, due to their ease of installation and use. They are also popular in commercial properties that offer wireless access to their employees and customers.

Norman Abramson, a professor at the University of Hawaii, developed the world's first wireless computer communication network, ALOHAnet. The system became operational in 1971 and included seven computers deployed over four islands to communicate with the central computer on the Oahu island without using phone lines.

54 Mbit/s WLAN PCI Card (802.11g)

Wireless LAN hardware initially cost so much that it was only used as an alternative to cabled LAN in places where cabling was difficult or impossible. Early development included industry-specific solutions and proprietary protocols, but at the end of the 1990s these were replaced by standards, primarily the various versions of IEEE 802.11 (in products using the Wi-Fi brand name). Beginning in 1991, a European alternative known as HiperLAN/1 was pursued by the European Telecommunications Standards Institute (ETSI) with a first version approved in 1996. This was followed by a HiperLAN/2 functional specification with ATM influences accomplished February 2000. Neither European standard achieved the commercial success of 802.11, although much of the work on HiperLAN/2 has survived in

the physical specification (PHY) for IEEE 802.11a, which is nearly identical to the PHY of HiperLAN/2.

In 2009 802.11n was added to 802.11. It operates in both the 2.4 GHz and 5 GHz bands at a maximum data transfer rate of 600 Mbit/s. Most newer routers are able to utilise both wireless bands, known as dualband. This allows data communications to avoid the crowded 2.4 GHz band, which is also shared with Bluetooth devices and microwave ovens. The 5 GHz band is also wider than the 2.4 GHz band, with more channels, which permits a greater number of devices to share the space. Not all channels are available in all regions.

A HomeRF group formed in 1997 to promote a technology aimed for residential use, but it disbanded at the end of 2002.

## Architecture

## Stations

All components that can connect into a wireless medium in a network are referred to as stations (STA). All stations are equipped with wireless network interface controllers (WNICs). Wireless stations fall into two categories: wireless access points, and clients. Access points (APs), normally wireless routers, are base stations for the wireless network. They transmit and receive radio frequencies for wireless enabled devices to communicate with. Wireless clients can be mobile devices such as laptops, personal digital assistants, IP phones and other smartphones, or non-portable devices such as desktop computers, printers, and workstations that are equipped with a wireless network interface.

**Basic service set**

The basic service set (BSS) is a set of all stations that can communicate with each other at PHY layer. Every BSS has an identification (ID) called the BSSID, which is the MAC address of the access point servicing the BSS.

There are two types of BSS: Independent BSS (also referred to as IBSS), and infrastructure BSS. An independent BSS (IBSS) is an ad hoc network that contains no access points, which means they cannot connect to any other basic service set.

Independent basic service set

An IBSS is a set of STAs configured in ad hoc (peer-to-peer)mode.

**Extended service set**

An extended service set (ESS) is a set of connected BSSs. Access points in an ESS are connected by a distribution system. Each ESS has an ID called the SSID which is a 32-byte (maximum) character string.

**Distribution system**

A distribution system (DS) connects access points in an extended service set. The concept of a DS can be used to increase network coverage through roaming between cells.

DS can be wired or wireless. Current wireless distribution systems are mostly based on WDS or MESH protocols, though other systems are in use.

Types of wireless LANs

The IEEE 802.11 has two basic modes of operation: infrastructure and ad hoc mode. In ad hoc mode, mobile units transmit directly peer-to-peer. In infrastructure mode, mobile units communicate through an access point that serves as a bridge to other networks (such as Internet or LAN).

Since wireless communication uses a more open medium for communication in comparison to wired LANs, the 802.11 designers also included encryption mechanisms: Wired Equivalent Privacy (WEP, now insecure), Wi-Fi Protected Access (WPA, WPA2, WPA3), to secure wireless computer networks. Many access points will also offer Wi-Fi Protected Setup, a quick (but now insecure) method of joining a new device to an encrypted network.

**Infrastructure**

Most Wi-Fi networks are deployed in infrastructure mode.

In infrastructure mode, a base station acts as a wireless access point hub, and nodes communicate through the hub. The hub usually, but not always, has a wired or fiber network connection, and may have permanent wireless connections to other nodes.

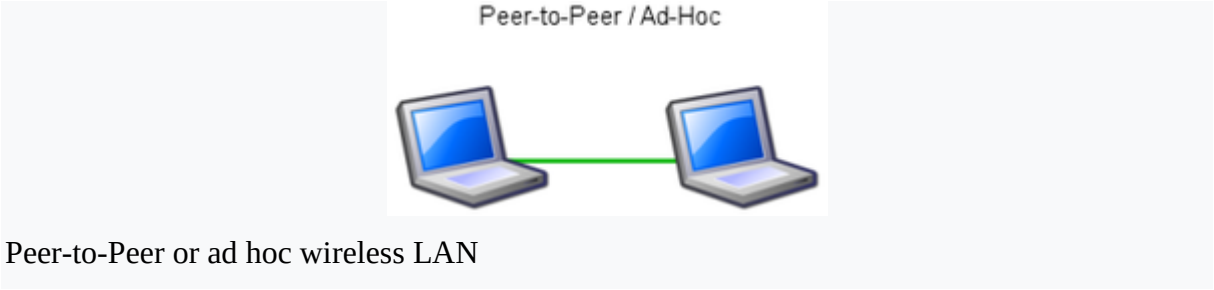
Wireless access points are usually fixed, and provide service to their client nodes within range.

Wireless clients, such as laptops, smartphones etc. connect to the access point to join the network.

Sometimes a network will have a multiple access points, with the same 'SSID' and security arrangement. In that case connecting to any access point on that network joins the client to the network. In that case, the client software will try to choose the access point to try to give the best service, such as the access point with the strongest signal.

**Peer-to-peer**

An ad hoc network (not the same as a WiFi Direct network is a network where stations communicate only peer to peer (P2P). There is no base and no one gives permission to talk. This is accomplished using the Independent Basic Service Set (IBSS).



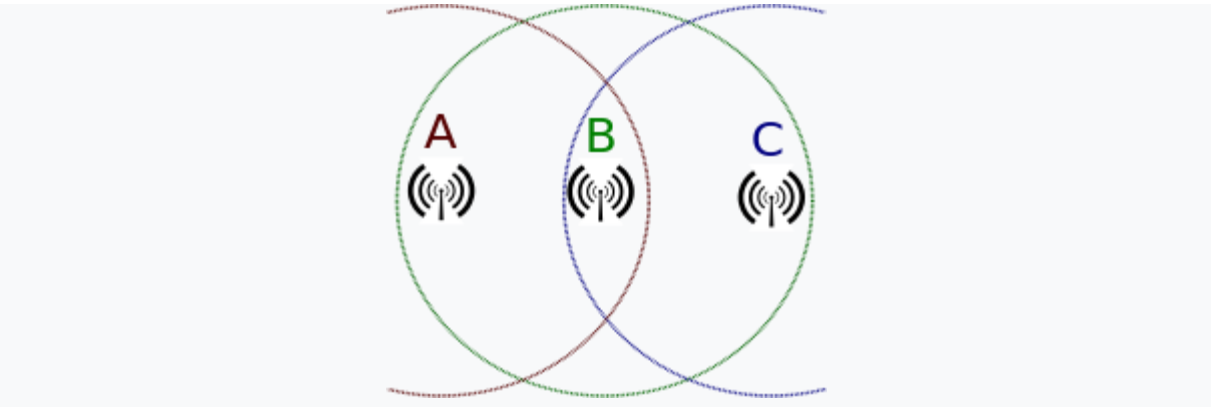

Peer-to-Peer or ad hoc wireless LAN

A WiFi Direct network is another type of network where stations communicate peer to peer.

In a Wi-Fi P2P group, the group owner operates as an access point and all other devices are clients. There are two main methods to establish a group owner in the Wi-Fi Direct group. In one approach, the user sets up a P2P group owner manually. This method is also known as Autonomous Group Owner (autonomous GO). In the second method, also called negotiation-based group creation, two devices compete based on the group owner intent value. The device with higher intent value becomes a group owner and the second device becomes a client. Group owner intent value can depend on whether the wireless device performs a cross-connection between an infrastructure WLAN service and a P2P group, remaining power in the wireless device, whether the wireless device is already a group owner in another group and/or a received signal strength of the first wireless device.

A peer-to-peer network allows wireless devices to directly communicate with each other. Wireless devices within range of each other can discover and communicate directly without involving central access points. This method is typically used by two computers so that they can connect to each other to form a network. This can basically occur in devices within a closed range.

If a signal strength meter is used in this situation, it may not read the strength accurately and can be misleading, because it registers the strength of the strongest signal, which may be the closest computer.




Hidden node problem: Devices A and C are both communicating with B, but are unaware of each other

IEEE 802.11 defines the physical layer (PHY) and MAC (Media Access Control) layers based on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). This is in contrast to Ethernet which uses CSMA-CD (Carrier Sense Multiple Access with Collision Detection). The 802.11 specification includes provisions designed to minimize collisions, because two mobile units may both be in range of a common access point, but out of range of each other.

**Bridge**

A bridge can be used to connect networks, typically of different types. A wireless Ethernet bridge allows the connection of devices on a wired Ethernet network to a wireless network. The bridge acts as the connection point to the Wireless LAN.

**Wireless distribution system**

A wireless distribution system (WDS) enables the wireless interconnection of access points in an IEEE 802.11 network. It allows a wireless network to be expanded using multiple access points without the need for a wired backbone to link them, as is traditionally required. The notable advantage of a WDS over other solutions is that it preserves the MAC addresses of client packets across links between access points.

An access point can be either a main, relay or remote base station. A main base station is typically connected to the wired Ethernet. A relay base station relays data between remote base stations, wireless clients or other relay stations to either a main or another relay base station. A remote base station accepts connections from wireless clients and passes them to relay or main stations. Connections between clients are made using MAC addresses rather than by specifying IP assignments.

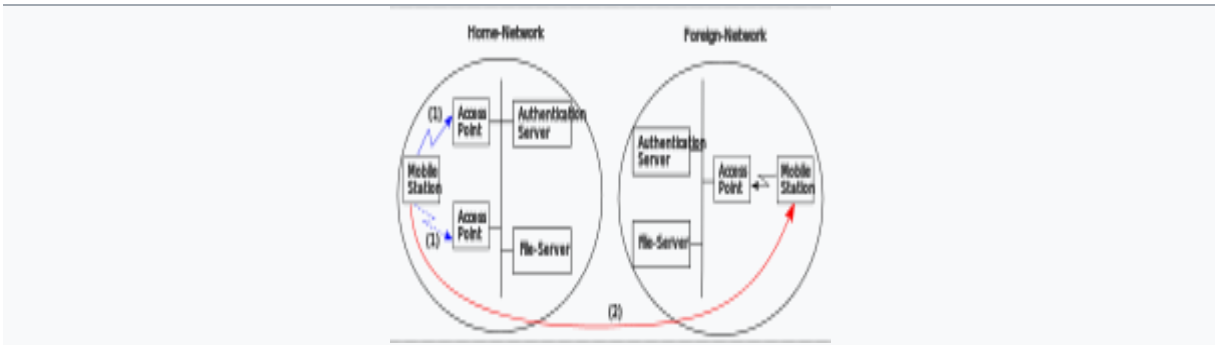
All base stations in a WDS must be configured to use the same radio channel, and share WEP keys or WPA keys if they are used. They can be configured to different service set identifiers.

WDS also requires that every base station be configured to forward to others in the system as mentioned above.

WDS capability may also be referred to as repeater mode because it appears to bridge and accept wireless clients at the same time (unlike traditional bridging). Throughput in this method is halved for all clients connected wirelessly.

When it is difficult to connect all of the access points in a network by wires, it is also possible to put up access points as repeaters.

**Roaming**




Roaming among Wireless Local Area Networks

There are two definitions for wireless LAN roaming:

1. **Internal roaming:** The Mobile Station (MS) moves from one access point (AP) to another AP within a home network if the signal strength is too weak. An authentication server (RADIUS) performs the re-authentication of MS via 802.1x (e.g. with PEAP). The billing of QoS is in the home network. A Mobile Station roaming from one access point to another often interrupts the flow of data among the Mobile Station and an application connected to the network. The Mobile Station, for instance, periodically monitors the presence of alternative access points (ones that will provide a better connection). At some point, based on proprietary mechanisms, the Mobile Station decides to re-associate with an access point having a stronger wireless signal. The Mobile Station, however, may lose a connection with an access point before associating with another access point. In order to provide reliable connections with applications, the Mobile Station must generally include software that provides session persistence.
2. **External roaming:** The MS (client) moves into a WLAN of another Wireless Internet Service Provider (WISP) and takes their services (Hotspot). The user can use a foreign network independently from their home network, provided that the foreign network allows

visiting users on their network. There must be special authentication and billing systems for mobile services in a foreign network.

**Applications**

Wireless LANs have a great deal of applications. Modern implementations of WLANs range from small in-home networks to large, campus-sized ones to completely mobile networks on airplanes and trains.

Users can access the Internet from WLAN hotspots in restaurants, hotels, and now with portable devices that connect to 3G or 4G networks. Oftentimes these types of public access points require no registration or password to join the network. Others can be accessed once registration has occurred and/or a fee is paid.

Existing Wireless LAN infrastructures can also be used to work as indoor positioning systems with no modification to the existing hardware.

**Benefits of WLAN**

What are the concrete benefits of WLAN over wired networks? While the most obvious is mobility, there are advantages also in building and maintaining a wireless network. Let us look at the benefits more closely:

**Mobility**

Mobility is a significant advantage of WLANs. User can access shared resources without looking for a place to plug in, anywhere in the organization. A wireless network allows users to be truly mobile as long as the mobile terminal is under the network coverage area.

**Range of coverage**

The distance over which RF and IR waves can communicate depends on product design (including transmitted power and receiver design) and the propagation path, especially in indoor environments. Interactions with typical building objects, such as walls, metal, and even people, can affect the propagation of energy, and thus also the range and coverage of the system. IR is blocked by solid objects, which provides additional limitations. Most wireless LAN systems use RF, because radio waves can penetrate many indoor walls and surfaces. The range of a typical WLAN node is about 100 m. Coverage can be extended, and true freedom of mobility achieved via roaming. This means using access points to cover an area in such a way that their coverages overlap each other. Thereby the user can wander around and move from the coverage area of one access point to another without even knowing he has, and at the same time seamlessy maintain the connection between his node and an access point.

**Ease of use**

WLAN is easy to use and the users need very little new information to take advantage of WLANs. Because the WLAN is transparent to a user's network operating system, applications work in the same way as they do in wired LANs.

**Installation Speed, Simplicity and Flexibility**

Installation of a WLAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings. Furthermore, wireless LAN enables networks to be set up where wires might be impossible to install.

**Scalability**

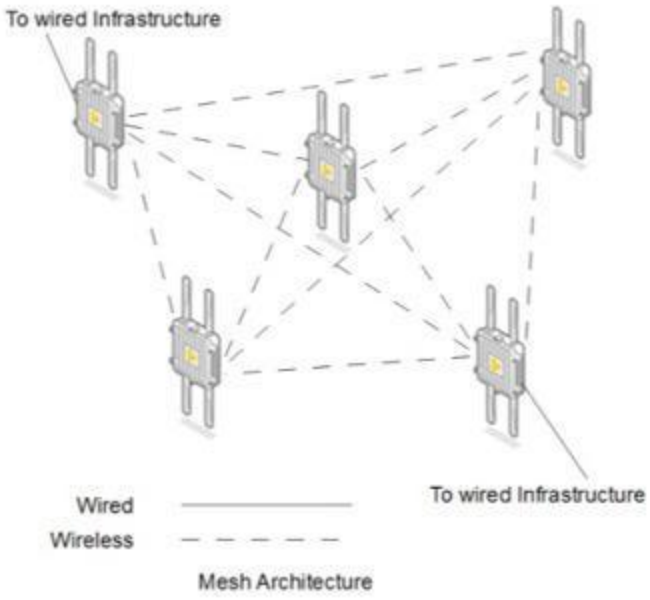
Wireless networks can be designed to be extremely simple or complex. Wireless networks can support large numbers of nodes and large physical areas by adding access points to extend coverage.

**Cost**

Finally, the cost of installing and maintaining a WLAN is on average lower than the cost of installing and maintaining a traditional wired LAN, for two reasons. First, WLAN eliminates the direct costs of cabling and the labor associated with installing and repairing it. Second, because WLANs simplify moving, additions, and changes, the indirect costs of user downtime and administrative overhead are reduced.

**WLAN topologies**

Industrial Wireless Tutorials: WLANs vary in the way communication is achieved and maintained including a basic service set, an extended service set, a mesh topology, and an ad hoc network. Learn how WLAN topologies and designs affect wireless performance.




As briefly discussed in our last segment on devices, WLANs vary in form and function according to specific needs. It makes sense, then, that WLANs vary in the way communication is achieved and maintained given the different scenarios. As we learned previously, a wireless network exists when RF is transmitted from the access point (AP), establishing a BSA; this is also known as the basic service set, or BSS. An AP begins by transmitting beacons, which advertise the characteristics of the BSS, such as channel, modulation scheme, and protocols supported.


The BSS is the basic building block of the wireless LAN. The BSS refers to the AP connected to the network infrastructure covering a finite area (the BSA) and handles all traffic to and from clients in that area. It may or may not be an infrastructure device, though

most stand-alone APs do function as a portal to the wired network, particularly if there is only one AP. The BSS allows a client to wirelessly communicate within the BSA and with other connected clients and network resources.

Expanding the network is accomplished by increasing power output or by the addition of APs. Raising output power brings with it several issues, while the addition of another AP can also create issues, so the design must be considered carefully. Raising output power is not always an option for APs, particularly those designed for the SOHO market. The concerns with raising power to expand the BSA are: first, client radios may be able to hear the access point, but the AP may not be able to hear the client; second, expanding the BSA will allow more client density in the BSA, creating more traffic and possible delays; third, raising power can cause interference with neighboring WLANs, or, as in the 5 gHz band, interference with radar systems at nearby airports.

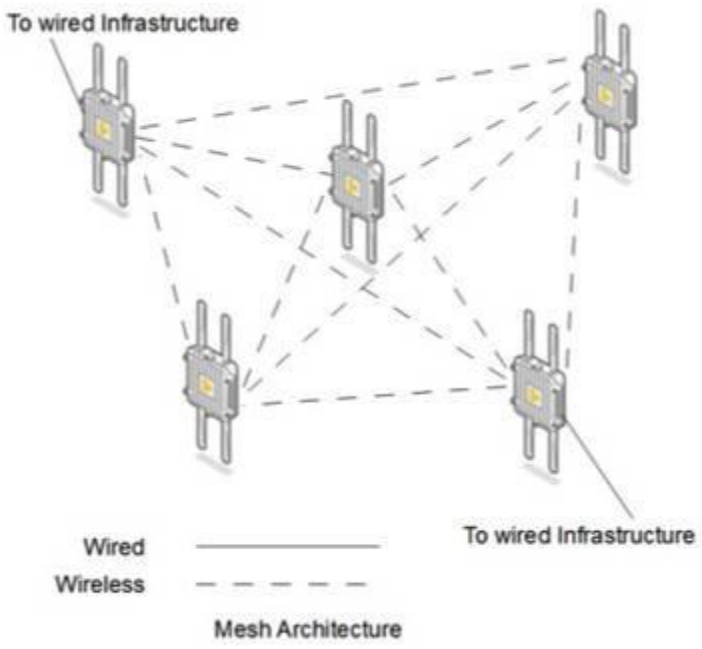
When adding APs, the first concern is interference. The new AP must not be on the same channel as the first. It must be assigned to a non-overlapping channel. This "co-channel" interference that could occur if APs are assigned the same channel will be discussed in a later segment. A multichannel architecture (MCA) must be perfected in order to allow proper coverage without excessive errors. The addition of another AP creates what is called an extended service set, or ESS. The ESS effectively expands the primary BSA by conjoining its BSA to the first point. The key to an ESS is proper configuration; aside from proper channel assignment, each of the APs in an ESS must also be configured with the same service set identifier (SSID) and password. As shown in the illustration, there must also be some overlap of the adjacent BSS-typically about 30%. This allows for uninterrupted roaming to occur between each BSS. Theoretically, a WLAN can be expanded indefinitely, observing proper channel assignment. However, a practical limit will be reached if an excessive number of "hops" between wireless APs occurs. It should be understood that roaming on an ESS is done through the wired infrastructure. Each new AP added to the ESS must be wired also. On a mesh type network, the backhaul is usually done wirelessly, but the same limitations apply.


In the above scenario, it is presumed that all, or the majority, of APs are infrastructure devices with a wired connection into the network. But what if you don't have the ability to wire every AP? What if the proposed coverage area is remote and has only power available? There are two ways to handle this problem: point-to-point (p2p) bridging and mesh topology. In the former, two radios are dedicated to the task of establishing a wireless link over a long distance. A good example is where two buildings on a campus are separated by several hundred feet, without any dedicated wiring or fiber between them. Typically, highly directional antennas are used to establish the link.

In a p2p link, one AP is the root node, while the other, or others, are non-root. This means that one node has control of the radio traffic, which avoids routing and quality of service (QoS) issues. Only one AP in a p2p link can be the root. It is possible to have multiple clients on this type of link: the root AP would broadcast over an omni-directional antenna, while the non-root, client nodes would use directional antennas aimed at the root antenna. Designing and implementing this type of network requires an understanding of local zoning laws governing antennas and towers, so don't overlook local considerations.

Another consideration, as you would expect, is the presence of obstacles or electromagnetic interference (EMI) in the path, or radio line of sight (RLOS). Over long distances, the Fresnel Zone must be calculated and plotted on a good quality topographic map; this will show elevations along the path, along with buildings, towers, and airports. However, the Fresnel Zone must not be obstructed by more than 40%, which means a physical survey of the path must be undertaken. For very long links longer than 7 miles, a phenomenon known as "earth bulge" must be considered. For a directional antenna at ground level, earth bulge becomes a problem at about 7 miles from the antenna. Raising the antenna to the top of a building or tower can mitigate this potential problem.

The other topology, mesh configuration, is more complicated. Very few vendors are capable of operating in a mesh configuration. In a mesh network, each AP cooperatively manages and controls the traffic between nodes. At least one node must be wired into the network infrastructure. This node is called the "mesh portal" and is the access point through which all network traffic accesses wired resources. In a properly designed mesh network, you need at least two portals. A single point of failure is not good practice. The book is still being written on best practice, but it is a good rule of thumb to limit four mesh APs to each portal. This can be further broken down to how many hops data needs to take between mesh APs.




While cooperative mesh points do a great job in routing and controlling data, it comes down the simple fact that the mesh APs operate like repeaters between themselves, and particularly for the mesh points that do not have a network association with the portal AP. This would require a client's traffic with the farthest AP (without portal association) to be forwarded to the nearest (lowest link cost) neighbor, which would forward or repeat the traffic to another portal until it reaches the portal AP. As we saw in the previous segment, repeating a signal comes with a significant cost in both signal strength and quality. Each hop can introduce 3 dB or more loss into the process; after three hops under ideal conditions, the signal may not be usable. Another good rule of thumb is to limit hops to two APs. This requires careful design that allows multiple paths to the mesh portals.

Mesh networks are essentially self-forming and self-healing, making them very robust. A mesh topology is also distributed in terms of control and data handling, making it an excellent

fit for use with distributed control systems. Even if the mesh portals are disabled, the network continues to operate, allowing for the transfer of data to continue between nodes. In a DCS, this loss of communication with the servers is not necessarily a problem in the short term; proper design would eliminate any single point of failure, such as a single mesh portal. Another consideration is the use of a WLAN controller in a controller-based network. A controller can also be a single point of failure in an otherwise robust wireless network. The pros and cons of controllers will be discussed in an upcoming segment.

One last network topology in common use is known as an independent basic service set, or IBSS. This type of network is also called an "ad hoc" network. An IBSS does not require an AP to operate. The network exists between mobile wireless devices and is typically set up "on the fly." Personal hotspots are an example of this type of network. This type of network is useful if there are several colleagues wishing to collaborate on a project without being exposed to a common wireless network in the office or being on an insecure public hotpot. Most operating systems allow for the setup of an ad hoc network using a wizard or some other utility.


An AD HOC Wireless network

In an ad hoc network, the SSID is the computer name or BSSID of the first device to begin sending beacons. Clients wishing to join the network would do so as with a BSS with the originating device controlling traffic and security. Caution must be exercised when using this method. If any of the networked computers has a simultaneous wired connection, this could provide an unauthorized path into the secure network environment. Security for an ad hoc network must be very robust, particularly in public venues. Data obtained by eavesdropping on these sessions can be very sensitive and create havoc for the entities involved in the ad hoc session.

**Different Types of Wireless Communication Technologies**

Wireless communication plays a significant role in day to day life. Besides communication, wireless technology has become an integral part of our daily activities. The transmission of data or information from one place to another wirelessly is referred as wireless communication. This provides an exchange of data without any conductor through RF and radio signals. The information is transmitted across the devices over some meters to hundreds of kilometres through well-defined channels.


Wireless Communication Technologies

Different types of signals are used in communication between the devices for wireless transmission of data. The following are the different electromagnetic signals are used depending on their wavelength and frequency.

- Radio Frequency Transmission
- Infrared Transmission
- Microwave Transmission
- Lightwave Transmission

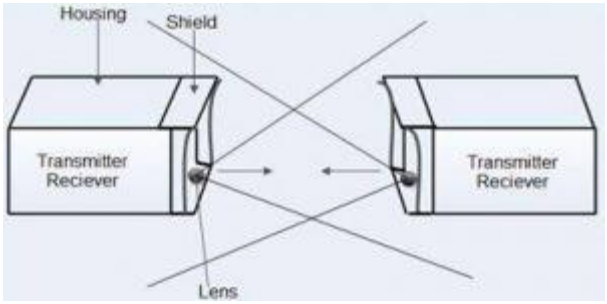
**Radio Frequency Transmission**

Radio frequency is a form of electromagnetic transmission used in wireless communication. RF signals are easily generated, ranging 3kHz to 300GHz. These are used in wireless communication because of their property to penetrate through objects and travel long distances.

Radio communication depends on the wavelength, transmitter power, receiver quality, type, size and height of the antenna.

**Drawbacks**

- These are frequency dependent
- These have the relatively low bandwidth for data transmission. Infrared Transmission
- Infrared radiations are electromagnetic radiations with longer wavelengths than visible light. These are usually used for short-range communications. These signals do not pass through solid objects.
- Examples like Television remote control, mobile data sharing.




Infrared Transmission

**Microwave Transmission**

Microwaves are the form of electromagnetic transmission used in wireless communication systems. The wavelength of microwave ranges from one meter to one millimetre. The frequency varies from 300MHz to 300GHz. These are widely used for long distance communications and are relatively less expensive.

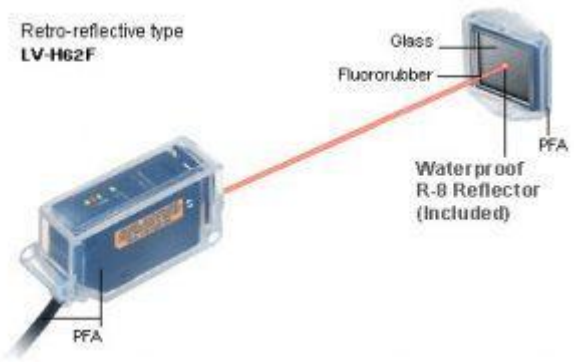
Microwave Transmission Node

**Drawbacks**

- The microwave does not pass through buildings.
- Bad weather affects the signal transmission.
- These are frequency dependent.

**Lightwave Transmission**

Light is an electromagnetic radiation with a wavelength ranging between infrared radiations and ultraviolet radiations. The wavelength ranges from 430 to 750THz. These are unguided optical signals such as laser and are unidirectional.




Lightwave Transmission

**Drawbacks**

- These signals cannot penetrate through rain and fog.
- The laser beam gets easily diverted by air.

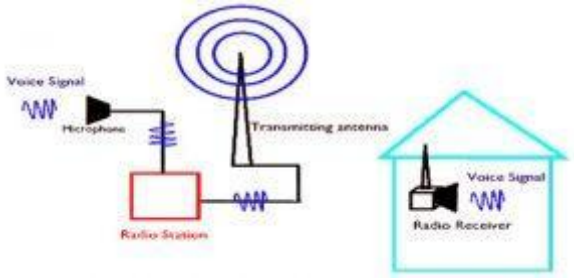
Types of Wireless Communication Technologies

Wireless communication technology is categorized into different types depending on the distance of communication, the range of data and type of devices used. The following are the different types of wireless communication technologies.

- Radio and Television Broadcasting
- Radar Communication
- Satellite communication
- Cellular Communication
- Global Positioning System
- WiFi
- Bluetooth
- Radio Frequency Identification

**Radio**

Radio communication was one of the first wireless technology developed and it is still in use. The portable multi-channel radios allow the user to communicate over short distances whereas citizen band and maritime radios provide communication services over long distances for truckers and sailors.



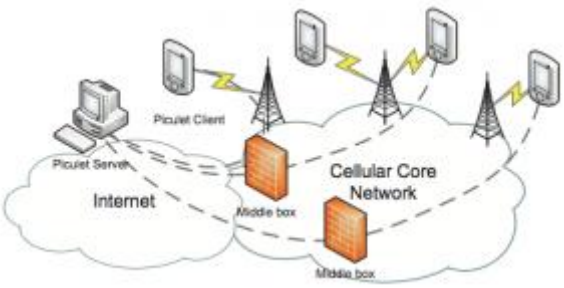

Radio Transmission

Mostly radio broadcasts sound through the air as radio waves. Radio has a transmitter which transmits the data in the form of radio signals to the receiver antenna.

To broadcast common programming stations are associated with the radio networks. The broadcast happens either in simulcast or syndication or both the forms. Radio broadcasting may be done via cable FM, and satellites over long distances at up to two megabits/Sec.

**Cellular**

A cellular network uses encrypted radio links, modulated to allow many users to communicate across the single frequency band. As the individual handsets lack significant broadcasting power, the system depends on a network of cellular towers which are capable of triangulating the source of any signal and handing reception duties off to the most suitable antenna.

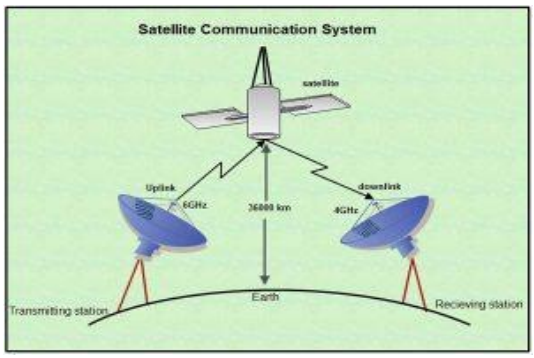



Cellular

The data transmission over cellular networks is possible with modern 4G systems capable of speeds reaching that of wired DSL. Cellular companies charge their customers by a minute of their voice and by the kilobytes for data.

**Satellite**

Satellite communication is a wireless technology having significant importance across the globe. They have found widespread use in specialized situations.




Satellite Communication System

The devices using satellite technology to communicate directly with the orbiting satellite through radio signals.

This allows users to stay connected virtually from anywhere on the earth. Portable satellite phones and modems have powerful broadcast feature and reception hardware than the cellular devices due to the increased range.

The satellite communication consists of a space segment and a ground segment. When the signal is sent to the satellite through a device, the satellite amplifies the signal and sent it back to the receiver antenna which is located on the earth's surface. The ground segment consists of a transmitter, receiver and the space segment, which is the satellite itself.

**Wi-Fi**

Wi-Fi is a low-cost wireless communication technology. A WiFi setup consists of a wireless router which serves a communication hub, linking portable device with an internet connection.This network facilitates connection of many devices depending on the router configuration. These networks are limited in range due to the low power transmission, allowing the user to connect only in the close proximity.

wi-fi

This network facilitates connection of many devices depending on the router configuration. These networks are limited in range due to the low power transmission, allowing the user to connect only in the close proximity.

**Advantages**

- Information can be transmitted quickly with a high speed and accuracy.
- The internet can be accessed from anywhere, at any time without any cables or wires.
- Emergency situations can be alerted through wireless communication.
- Wireless, no bunches of wire running out.
- Communication can reach where wiring is not feasible and costly.

**Disadvantages**

- An Unauthorized person can easily misuse the wireless signals which spread through the air.
- It is very important to secure the wireless network to protect information.
- High cost to set up the infrastructure.
- Wireless communication is influenced by physical constructions, climatic conditions and interference from other wireless devices.

  Applications Wireless Communication

  Wireless communication has wide applications.
- Space
- Military
- Telecommunications
- Wireless Power Transmission
- IoT

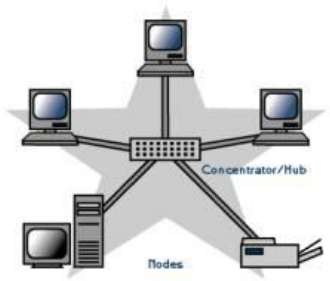
- Radar communication

Therefore, this is all about Types of wireless communication and applications, these networks are one of the important technologies in the telecommunications market. WiFi, WiMax, Bluetooth, Femtocell, 3G and 4G are some of the most important standards of Wireless technology.

The information which is given in this article will be helpful to the viewers. Furthermore, any queries, suggestions or electronics projects, you can comment us by commenting in the comment section below. Here is a question for you "What are the disadvantages of Wireless Communication?"

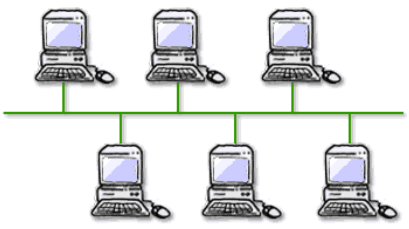
**Wired Networks**

Wired networks, also called Ethernet networks, are the most common type of local area network (LAN) technology. A wired network is simply a collection of two or more computers, printers, and other devices linked by Ethernet cables. Ethernet is the fastest wired network protocol, with connection speeds of 10 megabits per second (Mbps) to 100 Mbps or higher. Wired networks can also be used as part of other wired and wireless networks. To connect a computer to a network with an Ethernet cable, the computer must have an Ethernet adapter (sometimes called a network interface card, or NIC). Ethernet adapters can be internal (installed in a computer) or external (housed in a separate case). Some computers include a built-in Ethernet adapter port, which eliminates the need for a separate adapter (Microsoft). There are three basic network topologies that are most commonly used today. (Homenthelp.com)



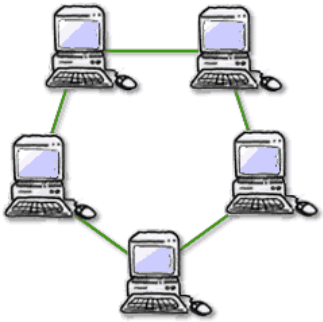

The star network, a general more simplistic type of topology, has one central hub that connects to three or more computers and the ability to network printers. This type can be used for small businesses and even home networks. The star network is very useful for applications where some processing must be centralized and some must be performed locally. The major disadvantage is the star network is its vulnerability. All data must pass through one central host computer and if that host fails the entire network will fail.

On the other hand the bus network has no central computer and all computers are linked on a single circuit. This type broadcasts signals in all directions and it uses special software to identify which



computer gets what signal. One disadvantage with this type of network is that only one signal can be sent at one time, if two signals are sent at the same time they will collide and the signal will fail to reach its destination. One advantage is that there is no central computer so if one computer goes down others will not be affected and will be able to send messages to one another. (Laudon)

The third type of network is the ring network. Similar to the bus network, the ring network does not rely on a central host computer either. Each computer in the network can communicate directly with any other computer, and each processes its own applications independently. A ring network forms a closed loop and data is sent in one direction only and if a computer in the network fails the data is still able to be transmitted.



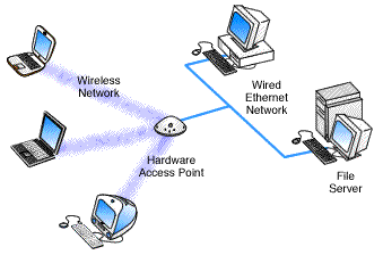
Typically the range of a wired network is within a 2,000-foot-radius. The disadvantage of this is that data transmission over this distance may be slow or nonexistent. The benefit of a wired network is that bandwidth is very high and that interference is very limited through direct connections. Wired networks are more secure and can be used in many situations; corporate LANs, school networks and hospitals. The biggest drawback to this type of network is that it must be rewired every time it is moved. (Laudon)

**Wireless Networks**

A wireless network, which uses high-frequency radio waves rather than wires to communicate between nodes, is another option for home or business networking. Individuals and organizations can use this option to expand their existing wired network or to go completely wireless. Wireless allows for devices to be shared without networking cable which increases mobility but decreases range. There are two main types of wireless networking; peer to peer or ad-hoc and infrastructure. (Wi-fi.com)

An ad-hoc or peer-to-peer wireless network consists of a number of computers each equipped with a wireless networking interface card. Each computer can communicate directly with all of the other wireless enabled computers. They can share files and printers this way, but may not be able to access wired LAN resources, unless one of the computers acts as a bridge to the wired LAN using special software.

An infrastructure wireless network consists of an access point or a base station. In this type of network the




access point acts like a hub, providing connectivity for the wireless computers. It can connect or bridge the wireless LAN to a wired LAN, allowing wireless computer access to LAN resources, such as file servers or existing Internet Connectivity. (compnetworking.about.com)

There are four basic types of transmissions standards for wireless networking. These types are produced by the Institute of Electrical and Electronic Engineers (IEEE). These standards define all aspects of radio frequency wireless networking. They have established four transmission standards; 802.11, 802.11a, 802.11b, 802.11g.

The basic differences between these four types are connection speed and radio frequency. 802.11 and 802.11b are the slowest at 1 or 2 Mbps and 5.5 and 11Mbps respectively. They both operate off of the 2.4 GHz radio frequency. 802.11a operates off of a 5 GHz frequency and can transmit up to 54 Mbps and the 802.11g operates off of the 2.4 GHz frequency and can transmit up to 54 Mbps. Actual transmission speeds vary depending on such factors as the number and size of the physical barriers within the network and any interference in the radio transmissions. (Wi-fi.com)

Wireless networks are reliable, but when interfered with it can reduce the range and the quality of the signal. Interference can be caused by other devices operating on the same radio frequency and it is very hard to control the addition of new devices on the same frequency. Usually if your wireless range is compromised considerably, more than likely, interference is to blame. (Laudon)

A major cause of interference with any radio signals are the materials in your surroundings, especially metallic substances, which have a tendency to reflect radio signals. Needless to say, the potential sources of metal around a home are numerous--things like metal studs, nails, building insulation with a foil backing and even lead paint can all possibly reduce the quality of the wireless radio signal. Materials with a high density, like concrete, tend to be harder for radio signals to penetrate, absorbing more of the energy. Other devices utilizing the same frequency can also result in interference with your wireless. For example, the 2.4GHz frequency used by 802.11b-based wireless products to communicate with each

other. Wireless devices don't have this frequency all to themselves. In a business environment, other devices that use the 2.4GHz band include microwave ovens and certain cordless phones. (Laundon)

On the other hand, many wireless networks can increase the range of the signal by using many different types of hardware devices. A wireless extender can be used to relay the radio frequency from one point to another without losing signal strength. Even though this device extends the range of a wireless signal it has some drawbacks. One drawback is that it extends the signal, but the transmission speed will be slowed.

There are many benefits to a wireless network. The most important one is the option to expand your current wired network to other areas of your organization where it would otherwise not be cost effective or practical to do so. An organization can also install a wireless network without physically disrupting the current workplace or wired network. (Wi-Fi.org) Wireless networks are far easier to move than a wired network and adding users to an existing wireless network is easy. Organizations opt for a wireless network in conference rooms, lobbies and offices where adding to the existing wired network may be too expensive to do so.

**Wired vs. Wireless Networking**

The biggest difference between these two types of networks is one uses network cables and one uses radio frequencies. A wired network allows for a faster and more secure connection and can only be used for distances shorter than 2,000 feet. A wireless network is a lot less secure and transmission speeds can suffer from outside interference. Although wireless networking is a lot more mobile than wired networking the range of the network is usually 150-300 indoors and up to 1000 feet outdoors depending on the terrain. (Homelanextream.com)

The cost for wired networking has become rather inexpensive. Ethernet cables, hubs and switches are very inexpensive. Some connection sharing software packages, like ICS, are free; some cost a nominal fee. Broadband routers cost more, but these are optional components of a wired network, and their higher cost is offset by the benefit of easier installation and built-in security features.

Wireless gear costs somewhat more than the equivalent wired Ethernet products. At full retail prices, wireless adapters and access points may cost three or four times as much as Ethernet cable adapters and hubs/switches, respectively. 802.11b products have dropped in price considerably with the release of 802.11g. (Homelanextream.com)

Wired LANs offer superior performance. A traditional Ethernet connection offers only 10 Mbps bandwidth, but 100 Mbps Fast Ethernet technology costs a little more and is readily available. Fast Ethernet should be sufficient for file sharing, gaming, and high-speed Internet access for many years into the future. (Wi-Fi.org) Wired LANs utilizing hubs can suffer performance slowdown if computers heavily utilize the network simultaneously. Use Ethernet switches instead of hubs to avoid this problem; a switch costs little more than a hub.

Wireless networks using 802.11b support a maximum bandwidth of 11 Mbps, roughly the same as that of old, traditional Ethernet. 802.11a and 802.11g LANs support 54 Mbps, that is approximately one-half the bandwidth of Fast Ethernet. Furthermore, wireless networking performance is distance sensitive, meaning that maximum performance will degrade on computers farther away from the access point or other communication endpoint. As more wireless devices utilize the 802.11 LAN more heavily, performance degrades even further. (Wi-Fi.org)

The greater mobility of wireless LANs helps offset the performance disadvantage. Mobile computers do not need to be tied to an Ethernet cable and can roam freely within the wireless network range. However, many computers are larger desktop models, and even mobile computers must sometimes be tied to an electrical cord and outlet for power. This undermines the mobility advantage of wireless networks in many organizations and homes.

For any wired network connected to the Internet, firewalls are the primary security consideration. Wired Ethernet hubs and switches do not support firewalls. However, firewall software products like Zone Alarm can be installed on the computers themselves. Broadband routers offer equivalent firewall capability built into the device, configurable through its own software.

In theory, wireless LANs are less secure than wired LANs, because wireless communication signals travel through the air and can easily be intercepted. The weaknesses of wireless security are more theoretical than practical. (Wi-Fi.org) Wireless networks protect their data through the Wired Equivalent Privacy (WEP) encryption standard that makes wireless communications reasonably as safe as wired ones.

No computer network is completely secure. Important security considerations for organizations tend to not be related to whether the network is wired or wireless but rather ensuring that the firewall is properly configured, employees are aware of the dangers of spoof emails, they are away of spy ware and how to avoid and that anyone outside the organization does not have unauthorized access to the network.

**Wireless Network Security**

Network security is a big concern for individuals and organizations because vital information is stored on the network and most critical process of the business are done through the network. If a network is to fail or security is compromised an organization could be completely crippled. For example, if Wal-Mart was to lose their cash register network than they would suffer a huge loss of business and would take, depending on the severity of the breach, several hours to days to fix.

Also at risk is employee and client privacy. If an organization's network is hacked into they would have access to client databases as well as employee databases. The most important thing to keep in mind when it comes to wireless network security is keeping unauthorized users from accessing your network. The first step is to know your wireless network's range and to use specific software to grant access only to authorized users.

# UNIT-III

# THE IEEE 802.11 STANDARD FOR WIRELESS LANS

A **wireless LAN** (**WLAN**) is a wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area such as a home, school, computer laboratory, campus, office building etc. This gives users the ability to move around within the area and yet still be connected to the network. Through a gateway, a WLAN can also provide a connection to the wider Internet.

Most modern WLANs are based on IEEE 802.11 standards and are marketed under the Wi-Fi brand name.

Wireless LANs have become popular for use in the home, due to their ease of installation and use. They are also popular in commercial properties that offer wireless access to their employees and customers.

Wireless LAN (WLAN) that is to say, "Wireless LAN", not to be confused with WAN course. Also referred Radio LAN (WLAN) if the communication medium is the radio (not light infrared for example).The stations of the wireless network can communicate directly with each other, we called Ad Hoc network type, or via relay terminals called APs (Access Points, PA) then it is an infrastructure network. the second type is by far the most common in business.

The wired LAN provides reliable service to users, working in a fixed environment. Once installed, the workstations and the servers of a wired LAN are fixed in their native locations. For users who are highly mobile or in a rough terrain, where there is no possibility to install and lay down the cables of a wired LAN, a good solution is to install a wireless LAN. Wireless LANs transmit and receive data over the atmosphere, using radio frequency (RF) or infrared optical technology, there by, eliminating the need for fixed wired connections. Wireless LANs provides dual advantage of connectivity and mobility. Wireless LANs have gained strong popularity in applications like health-care, retail, manufacturing, warehousing, and academic. These applications use hand-held terminals and notebook computers to transmit real-time information to centralized 'hosts' for processing. Figure shows simple wired and wireless networks.

Wireless LANs have limitations when compared with wired LANs. Wireless LANs are slower than wired LAN. Also, they have limitations with their range of operation. When a station is moved out of its range, it suffers from noise and error in the received data due to the poor signal strength.

IEEE formed a working group to develop a Medium Access Control (MAC) and Physical Layer (PHY) standard for wireless connectivity for stationary, portable, and mobile computers within a local area. This working group is IEEE 802.11. The recommendations of the 802.11 committee have become the standard for wireless networking.

## Need for Wireless LANs

Networking and Internet services are essential requirements for today's business computing. An increasing number of LAN users are becoming mobile. These mobile users require connectivity to a network, regardless of where they are because they want simultaneous access to the network. With wireless LANs, users can access shared information without looking for a place to plug in their systems and do not need network managers to set up networks to install cable and other equipment.

## Advantages of Wireless LANs

Wireless LANs offer the following advantages over traditional wired networks. Mobility Users on a wireless LAN systems can access to real-time information from anywhere within their organization. This mobility supports productivity and service opportunities, which are not possible with wired networks.

Fast Installation and Simplicity: Installing a wireless LAN system can be fast and easy and can eliminate the need to pull cables through walls, floor, and ceilings.

Installation Flexibility: Wireless network is suitable for any kind of geographical conditions. Installation requires to properly setup the transmitter and the receiver antenna (RF) or infrared system. This is much easier than cable installation of a wired LAN. If a company decided to move to a new location, the wireless system is much easier to move.

Reduced Cost: The initial investment required for wireless LAN hardware is higher than the cost of wired LAN hardware. However, the overall installation expenses and life cycle costs are significantly lower. Long-term cost benefits are greatest in dynamic environments, requiring frequent moves and changes.

Scalability Wireless LAN systems can be configured in a variety of topologies to cater to the need for specific applications and installations. Configurations can be easily changed. They scale well. New nodes can be added to the existing wireless LAN without much degradation of performance.

## Uses of Wireless LANs

- Wireless LANs frequently act as a substitute rather than replacement for a wired LAN network. They often provide the final few meters of connectivity between a wired network and the mobile user. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs:
- Doctors and nurses in hospitals can be more productive because wireless hand-held terminals or notebook computers with wireless LAN capability can deliver patient information instantly.
- Consulting or accounting audit teams or small workgroups can increase the productivity with quick wireless network setup.
- Students or research scholars, attending a class inside an institute campus can instantly access the Internet to consult the catalog of the net digital library.
- Network managers in dynamic environments minimize the overhead caused by moves, extensions to networks, and other changes with wireless LANs.
- Training sites at corporations and students at universities use wireless connectivity to ease access to information, information exchanges, and learning.
- Network managers installing networked computers in older buildings find that wireless LANs are a cost-effective network infrastructure solution.
- Travelers and tourists can book their ticket through the net during their travel.
- Warehouse workers use wireless LANs to exchange information with central databases.
- Network managers implement wireless LANs to provide backup for mission-critical applications, running on wired networks.
- Senior executives in meetings make quicker decisions because they have real-time information at their fingertips.

## Component of a Wireless LAN

Apart from the components needed by the conventional wired LAN, a wireless LAN needs additional components. They are the transmitters and receivers at radio frequency (RF) or

infrared (IR). The RF transmitter and receivers need antennas to perform two-way communication. This area requires a wide knowledge about antenna and propagation. Usually a trial installation is carried out before actual implementation. Hubs, bridges, network operating system, servers, and other components are functioning exactly as they were, on a wired LAN.

## Mobile Clients

Mobile clients are portable computing devices that act as clients. The following are some of the mobile systems.

1. Laptop computers: Laptop PCs with two-way communication facility (Transceiver)
2. Palmtops or Personal Digital Assistants (PDA) with communication capability
3.PortableFAX
4. Cellular phones

Special Units

For network management and efficient communication, a wireless LAN needs additional equipments.
They are:

Communication units: These units perform communications within the network and also with other networks.

Data collecting units: These units collect data from other systems.

Security Units: These units take care of the network security.

Transceivers: A transceiver is a half-duplex device. It performs transmission and reception of data within a wireless LAN. It can be able to transmit in one direction at a time.

Portable bridges: Portable Bridge can support internet working functions. Two wireless LANs can communicate with each other using a bridge. It can be a transceiver or a satellite port or other communication unit that provides a bridge service.

## Working of Wireless LANs

Wireless LANs use electromagnetic waves (radio or infrared technology) to communicate information from one point to another without relying on any physical connection. Radio waves are often referred as radio carriers because they simply perform the function of delivering energy to a remote receiver. The data being transmitted is superimposed on the

radio carrier so that it can be accurately extracted at the receiving end. This is generally referred to as modulation of the carrier by the information being transmitted. Once data is superimposed (modulated) onto the radio carrier, the radio signal occupies more than a single frequency, since the frequency or bit rate of the modulating information adds to the carrier. Multiple radio carriers can exist in the same space at the same time without interfering with each other if the radio waves are transmitted on different radio frequencies. To extract data, a radio receiver tunes in one radio frequency while rejecting all other frequencies. In a typical wireless LAN configuration, a transmitter/receiver (transceiver) device, called an access point, connects to the wired network from a fixed location, using standard cabling. The access point receives, buffers, and retransmits data between the wireless LAN and the wired network infrastructure. A single access point can support a small group of users and can function within a range of less than one hundred to several hundred feet. The access point (or the antenna attached to the access point) is usually mounted high but may be mounted essentially anywhere that is practical as long as the desired radio coverage is obtained.

End users access the wireless LAN through wireless LAN adapters, which are implemented as add-on cards in notebook or palmtop computers, as cards in desktop computers, or integrated within hand-held computers. Wireless LAN adapters provide an interface between the client network operating system (NOS) and the airwaves via an antenna. The nature of the wireless connection is transparent to the NOS.

**There are two types of wireless networks:**

• Type networks Ad Hoc, where stations communicate directly;
• Infrastructure type networks where stations communicate through access points.

To communicate, each station must of course be equipped with an adapter WiFi and a radio antenna (often integrated into the adapter). More and more computer equipment come with a built-in WiFi adapter. Except not the case, you must buy one and connect it to the station. The connection is very varied: there are WiFi USB adapters, PCMCIA, PCI, etc. There are several variations of WiFi. In short, 802.11b and 802.11g are compatible them and both operate with the radio waves of a frequency of 2.4 GHz. The 802.11b reached a speed of 11 Mb / s and 802.11g rises to 54 Mb / s. The 802.11a is not compatible with 802.11b and 802.11g, because it works with the waves a radio frequency of 5 GHz. It can reach 54 Mb / s. The 802.11n allows to achieve a real flow rate greater than 100 Mb / s. It is capable of operating at 2.4 GHz or 5 GHz and is compatible with the 802.11b / g and 802.11a.

Unfortunately, Most 802.11n equipment available today use only tape 2.4 GHz (and are therefore not compatible with the 802.11a).
Today the WiFi version of the most used is far 802.11g. It should be rapidly overtaken by 802.11n.

The fact that WiFi is originally designed to perform WLAN does not prevent not also be used in other contexts. For example, a myriad of products, such as electronic organizers (PDAs) or Personal Data Assistant (PDAs), printers, computer monitors, VCRs or even Hi-Fi, are now equipped with WiFi connections allowing them to be linked together without any wire. In this case, the WLAN is used to achieve a WPAN. Conversely, many local authorities do not have access to top speed (ADSL is not available everywhere) are turning to WiFi to cover a town or towns with the same wireless network. This can be called Wireless MAN (WMAN). Finally, companies are deploying wireless networks, called hotspots1 that allow anyone to connect to the Internet wirelessly slightly across the US and around the world. So one sees now what might be called WWAN (Wireless Wide Area Networks) based on WiFi technology (WiFi technology itself, however, carries data over short distances).

## 802.11 Architecture

The 802.11architecture defines two types of services and three different types of stations

802.11 Services

The two types of services are

1. Basic services set (BSS)

2. Extended Service Set (ESS)

1. Basic Services Set (BSS)

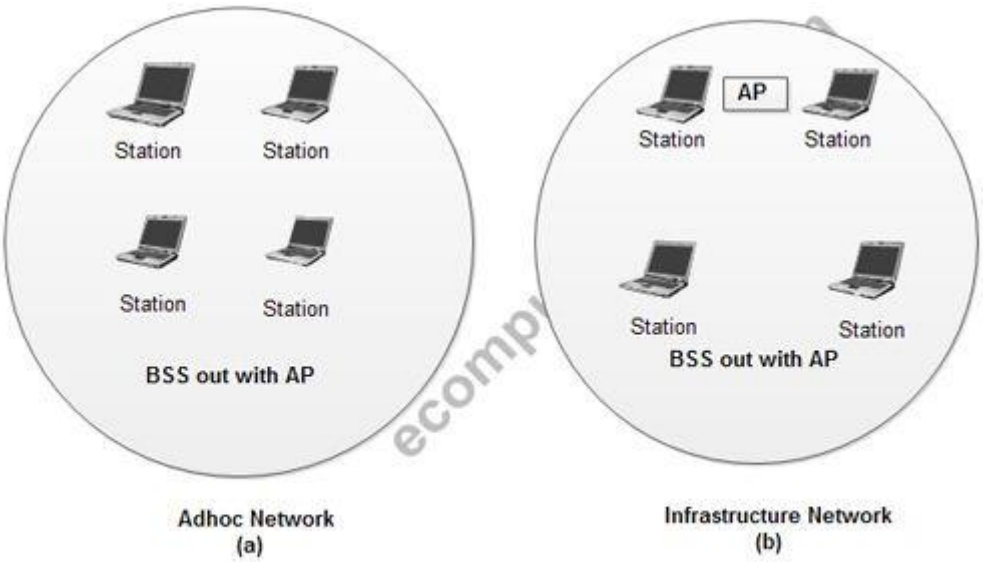
• The basic services set contain stationary or mobile wireless stations and a central base station called access point (AP).

• The use of access point is optional.

• If the access point is not present, it is known as stand-alone network. Such a

BSS cannot send data to other BSSs. This type of architecture is known as adhoc architecture.

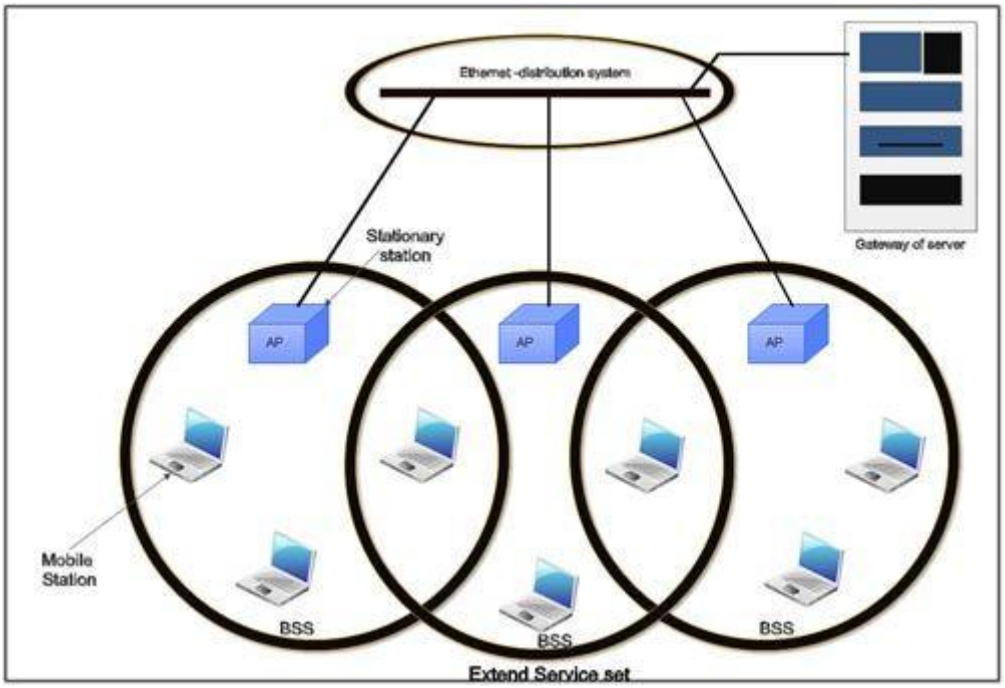
• The BSS in which an access point is present is known as an infrastructure network.




**Basic Service Sets**

2. Extend Service Set (ESS)

• An extended service set is created by joining two or more basic service sets (BSS) having access points (APs).




• These extended networks are created by joining the access points of basic services sets through a wired LAN known as distribution system.

• The distribution system can be any IEET LAN.

• There are two types of stations in ESS:

(i) Mobile stations: These are normal stations inside a BSS.

(ii) Stationary stations: These are AP stations that are part of a wired LAN.

• Communication between two stations in two different BSS usually occurs via two APs.

• A mobile station can belong to more than one BSS at the same time.

**802.11 Station Types**

IEEE 802.11 defines three types of stations on the basis of their mobility in wireless LAN. These are:

1. No-transition Mobility

2. BSS-transition Mobility

3. ESS-transition Mobility

1. No-transition .Mobility: These types of stations are either stationary i.e. immovable or move only inside a BSS.

2. BSS-transition mobility: These types of stations can move from one BSS to another but the movement is limited inside an ESS.

3. ESS-transition mobility: These types of stations can move from one ESS to another. The communication mayor may not be continuous when a station moves from one ESS to another ESS.

**Physical layer functions**

• As we know that physical layer is responsible for converting data stream into signals, the bits of 802.11 networks can be converted to radio waves or infrared waves.

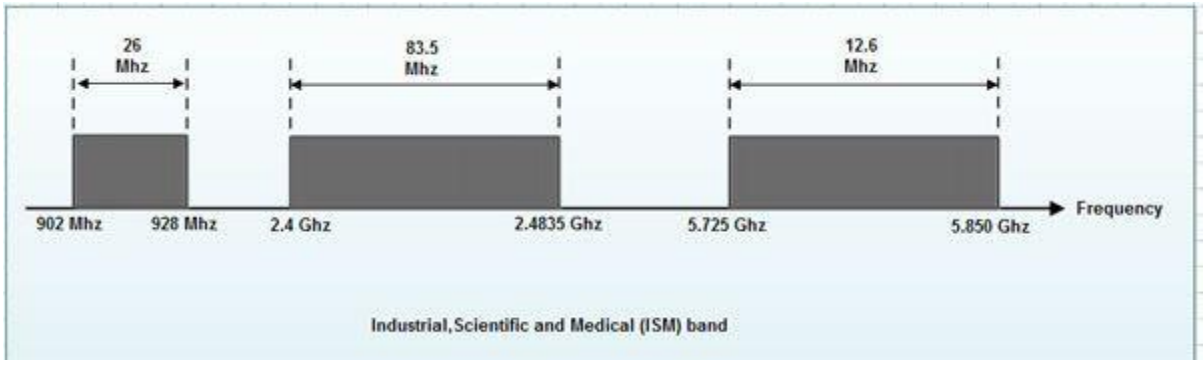
• These are six different specifications of IEEE 802.11. These implementations, except the first one, operate in industrial, scientific and medical (ISM) band. These three banks are unlicensed and their ranges are

1.902-928 MHz

2.2.400-4.835 GHz

3.5.725-5.850

GHz




• **The different implementations of IEE802.11 are given below:**

**1. IEEE 802.11 infrared**

• It uses diffused (not line of sight) infrared light in the range of 800 to 950 nm.

• It allows two different speeds: I Mbps and 2Mbps.

• For a I-Mbps data rate, 4 bits of data are encoded into 16 bit code. This 16 bit code contains fifteen as and a single 1.

• For a 2-Mbps data rate, a 2 bit code is encoded into 4 bit code. This 4 bit code contains three Os and a single 1.

• The modulation technique used is pulse position modulation (PPM) i.e. for converting digital signal to analog.

**2. IEEE 802.11 FHSS**

• IEEE 802.11 uses Frequency Hoping Spread Spectrum (FHSS) method for signal generation.

• This method uses 2.4 GHz ISM band. This band is divided into 79 subbands of 1MHz with some guard bands.

• In this method, at one moment data is sent by using one carrier frequency and then by some other carrier frequency at next moment. After this, an idle time is there in communication. This cycle is repeated after regular intervals.

• A pseudo random number generator selects the hopping sequence.

• The allowed data rates are 1 or 2 Mbps.

• This method uses frequency shift keying (two level or four level) for modulation i.e. for converting digital signal to analogy.

**3. IEEE 802.11 DSSS**

• This method uses Direct Sequence Spread Spectrum (DSSS) method for signal generation. Each bit is transmitted as 11 chips using a Barker sequence.

• DSSS uses the 2.4-GHz ISM band.

• It also allows the data rates of 1 or 2 Mbps.

• It uses phase shift keying (PSK) technique at 1 M baud for converting digital signal to analog signal.

**4. IEEE 802.11a OFDM**

• This method uses Orthogonal Frequency Division Multiplexing (OFDM) for signal generation.

• This method is capable of delivering data upto 18 or 54 Mbps.

• In OFDM all the subbands are used by one source at a given time.

• It uses 5 GHz ISM band.

• This band is divided into 52 subbands, with 48 subbands for data and 4 subbands for control information.

• If phase shift keying (PSK) is used for modulation then data rate is 18 Mbps. If quadrature amplitude modulation (QAM) is used, the data rate can be 54 Mbps.

**5. IEEE 802.11b HR-OSSS**

• It uses High Rate Direct Sequence Spread Spectrum method for signal generation.

• HR-DSSS is similar to DSSS except for encoding method.

• Here, 4 or 8 bits are encoded into a special symbol called complementary code key (CCK).

• It uses 2.4 GHz ISM band.

• It supports four data rates: 1,2,5.5 and 11 Mbps.

• 1 Mbps and 2 Mbps data rates uses phase shift modulation.

• The 5.5. Mbps version uses BPSK and transmits at 1.375 Mbaud/s with 4-bit CCK encoding.

• The 11 Mbps version uses QPSK and transmits at 1.375 Mbps with 8-bit CCK encoding.

**6. IEEE 802.11g OFDM**

• It uses OFDM modulation technique.

• It uses 2.4 GHz ISM band.

• It supports the data rates of 22 or 54 Mbps.

• It is backward compatible with 802.11 b.

MAC sublayer Functions

802.11 support two different modes of operations. These are:

1. Distributed Coordination Function (DCF)

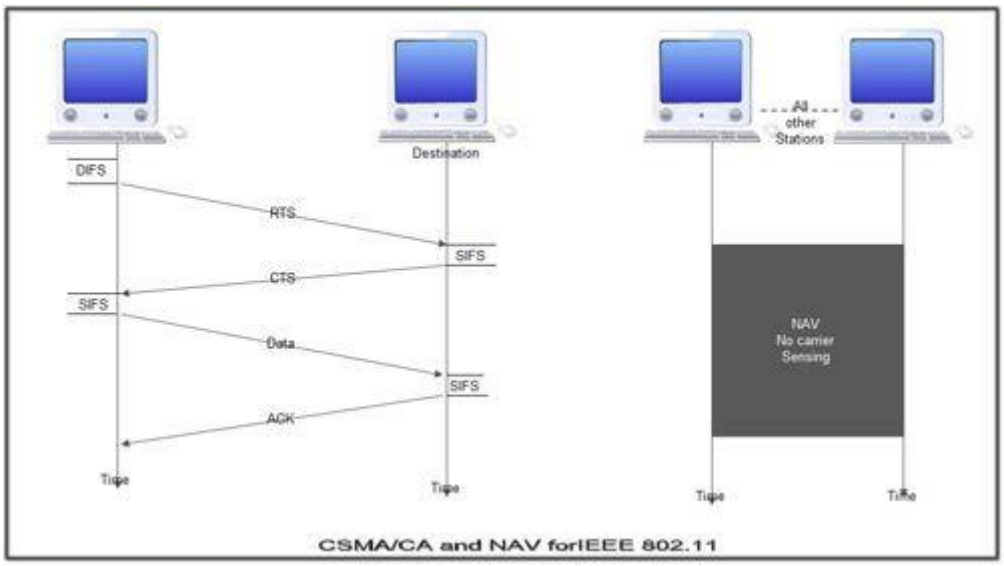
2. Point Coordination Function (PCF)

1. Distributed Coordination Function

• The DCF is used in BSS having no access point.

• DCF uses CSMA/CA protocol for transmission.

• The following steps are followed in this method.



CSMA/CA and NAV forIEEE 802.11

1. When a station wants to transmit, it senses the channel to see whether it is free or not.

2. If the channel is not free the station waits for back off time.

3. If the station finds a channel to be idle, the station waits for a period of time called distributed interframe space (DIFS).

4. The station then sends control frame called request to send (RTS) as shown in figure.

5. The destination station receives the frame and waits for a short period of time called short interframe space (SIFS).

6. The destination station then sends a control frame called clear to send (CTS) to the source station. This frame indicates that the destination station is ready to receive data.

7. The sender then waits for SIFS time and sends data.

8. The destination waits for SIFS time and sends acknowledgement for the received frame.

Collision avoidance

• 802.11 standard uses Network Allocation Vector (NAV) for collision avoidance.

• The procedure used in NAV is explained below:

1. Whenever a station sends an RTS frame, it includes the duration of time for which the station will occupy the channel.

2. All other stations that are affected by the transmission creates a timer caned network allocation vector (NAV).

3. This NAV (created by other stations) specifies for how much time these stations must not check the channel.

4. Each station before sensing the channel, check its NAV to see if has expired or not.

5. If its NA V has expired, the station can send data, otherwise it has to wait.

• There can also be a collision during handshaking i.e. when RTS or CTS control frames are exchanged between the sender and receiver. In this case following procedure is used for collision avoidance:

1. When two or more stations send RTS to a station at same time, their control frames collide.

2. If CTS frame is not received by the sender, it assumes that there has been a collision.

3. In such a case sender, waits for back off time and retransmits RTS.

2. Point Coordination Function

• PCF method is used in infrastructure network. In this Access point is used to control the network activity.

• It is implemented on top of the DCF and IS used for time sensitive transmissions.

• PCF uses centralized, contention free polling access method.

• The AP performs polling for stations that wants to transmit data. The various stations are polled one after the other.

• To give priority to PCF over DCF, another interframe space called PIFS is defined. PIFS (PCF IFS) is shorter than DIFS.

• If at the same time, a station is using DCF and AP is using PCF, then AP is given priority over the station.

• Due to this priority of PCF over DCF, stations that only use DCF may not gain access to the channel.

• To overcome this problem, a repetition interval is defined that is repeated continuously. This repetition interval starts with a special control frame called beacon frame.

• When a station hears beacon frame, it start their NAV for the duration of the period of the repetition interval.

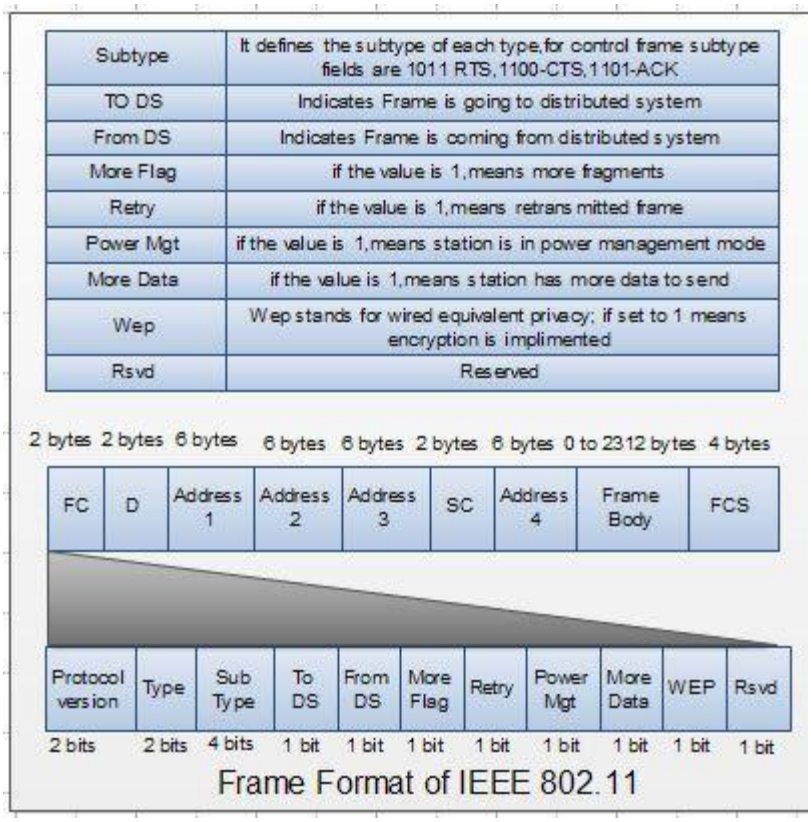
Frame Format of 802.11

The MAC layer frame consists of nine fields.

1. Frame Control (FC). This is 2 byte field and defines the type of frame and some control information. This field contains several different subfields.

These are listed in the table below:

| Field | Explanation |
|---|---|
| Version | The Current Version is 0. |
| Type | Specifies the type of information in the frame body 00-Management,01-control,and 10-Data. |




2. D. It stands for duration and is of 2 bytes. This field defines the duration for which the frame and its acknowledgement will occupy the channel. It is also used to set the value of NA V for other stations.

3. Addresses. There are 4 address fields of 6 bytes length. These four addresses represent source, destination, source base station and destination base station.

4. Sequence Control (SC). This 2 byte field defines the sequence number of frame to be used in flow control.

5. Frame body. This field can be between 0 and 2312 bytes. It contains the information.

6. FCS. This field is 4 bytes long and contains 'cRC-32 error detection sequence.

**IEEE 802.11 Frame types**

There are three different types of frames:

1. Management frame

2. Control frame

3. Data frame

1. Management frame. These are used for initial communication between stations and access points.

2. Control frame. These are used for accessing the channel and acknowledging frames. The control frames are RTS and CTS.

3. Data frame. These are used for carrying data and control information.

802.11 Addressing

• There are four different addressing cases depending upon the value of To DS And from DS subfields of FC field.

• Each flag can be 0 or 1, resulting in 4 different situations.

1. If To DS = 0 and From DS = 0, it indicates that frame is not going to distribution system and is not coming from a distribution system. The frame is going from one station in a BSS to another.

2. If To DS = 0 and From DS = 1, it indicates that the frame is coming from a distribution system. The frame is coming from an AP and is going to a station. The address 3 contains original sender of the frame (in another BSS).

3. If To DS = 1 and From DS = 0, it indicates that the frame is going to a distribution system. The frame is going from a station to an AP. The address 3 field contains the final destination of the frame.

4. If To DS = 1 and From DS = 1,it indicates that frame is going from one AP to another AP in a wireless distributed system.

The table below specifies the addresses of all four cases.

| TO DS | From DS | Address 1 | Address 2 | Address3 | Addres 4 |
|---|---|---|---|---|---|
| 0 | 0 | Destination | Source | BSS ID | N/A |
| 0 | 1 | Destination | Sending AP | Source | N/A |
| 1 | 0 | Receiving AP | Source | Destination | N/A |
| 1 | 1 | Receiving AP | Sending AP | Destination | Source |

**Protocols for Wireless LAN**

The CSMA protocol is very difficult to implement for wireless LAN. Hence special protocols are needed to avoid collision. MACA and MACAW are the two widely used protocols.

**MACA Protocol**

During 1990, Kam developed the MACA (Multiple Access with Collision Avoidance) protocol for wireless transmission. The protocol is very simple to implement and works in the following manner. Station X, willing to transmit data to the nearby station Y, sends a short frame called RTS (Request to Send) first. On hearing this short frame, all stations other than the receiving station, avoid transmission, thereby allowing the communication to take place without interference. The receiving station sends a CTS (Clear to Send) frame to the calling station. After receiving the CTS frame, station X begins transmission. When simultaneous transmission of RTS by two stations Wand X to station Y occurs, both frames collide with each other and are lost. When there is no CTS from station Y, both stations wait for a random amount of time (binary exponential back off) and start the whole process again.

**MACAW Protocol**

Bhargavan et al (1994) investigated the behavior of MACA protocol and refined it with modifications. The first modification was the acknowledgment frame for the successful receipt of each frame. This modification adds carrier sense to stations. The second modification was to apply the binary exponential back off algorithm to source-destination pair. This improves the fairness of the protocol. They have also added to stations, the ability to exchange information, regarding congestion.

# UNIT-IV

# WIRELESS PANS

LAN technology enables device connectivity to infrastructure based services through a wireless carrier provider. The need for personal devices to communicate wirelessly with one another without an established infrastructure has led to the emergence of Personal Area Networks (PANs).

- Ericsson's Bluetooth project in 1994 defines the standard for PANs to enable communication between mobile phones using low power and low cost radio interfaces.
- In May 1988, Companies such as IBM, Intel, Nokia and Toshiba joined Ericsson to form the Bluetooth Special Interest Group (SIG) whose aim was to develop a defacto standard for PANs.
- IEEE has approved a Bluetooth based standard named IEEE 802.15.1 for Wireless Personal Area Networks (WPANs). IEEE standard covers MAC and Physical layer applications.

Bluetooth specification details the entire protocol stack. Bluetooth employs Radio Frequency (RF) for communication. It makes use of frequency modulation to generate radio waves in the ISM band.

Symbol of Bluetooth

An example of a Bluetooth device

The usage of Bluetooth has widely increased for its special features.

- Bluetooth offers a uniform structure for a wide range of devices to connect and communicate with each other.

- Bluetooth technology has achieved global acceptance such that any Bluetooth enabled device, almost everywhere in the world, can be connected with Bluetooth enabled devices.
- Low power consumption of Bluetooth technology and an offered range of up to ten meters has paved the way for several usage models.
- Bluetooth offers interactive conference by establishing an adhoc network of laptops.
- Bluetooth usage model includes cordless computer, intercom, cordless phone and mobile phones.

Piconets and Scatternets

Bluetooth enabled electronic devices connect and communicate wirelessly through shortrange devices known as Piconets. Bluetooth devices exist in small ad-hoc configurations with the ability to act either as master or slave the specification allows a mechanism for master and slave to switch their roles. Point to point configuration with one master and one slave is the simplest configuration.

When more than two Bluetooth devices communicate with one another, this is called a PICONET. A Piconet can contain up to seven slaves clustered around a single master. The device that initializes establishment of the Piconet becomes the master.

The master is responsible for transmission control by dividing the network into a series of time slots amongst the network members, as a part of time division multiplexing scheme which is shown below.

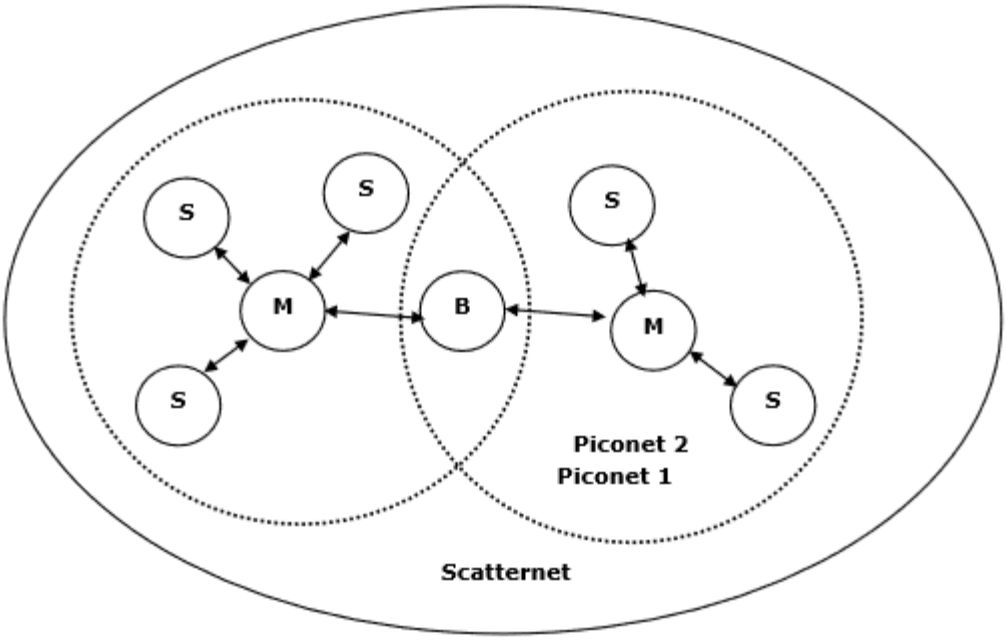



**Figure: Piconets and Scatternets**

The features of Piconets are as follows −

- Within a Piconet, the timing of various devices and the frequency hopping sequence of individual devices is determined by the clock and unique 48-bit address of master.
- Each device can communicate simultaneously with up to seven other devices within a single Piconet.
- Each device can communicate with several piconets simultaneously.
- Piconets are established dynamically and automatically as Bluetooth enabled devices enter and leave piconets.
- There is no direct connection between the slaves and all the connections are essentially master-to-slave or slave-to-master.
- Slaves are allowed to transmit once these have been polled by the master.
- Transmission starts in the slave-to-master time slot immediately following a polling packet from the master.
- A device can be a member of two or more piconets, jumping from one piconet to another by adjusting the transmission regime-timing and frequency hopping sequence dictated by the master device of the second piconet.

- It can be a slave in one piconet and master in another. It however cannot be a master in more than once piconet.
- Devices resident in adjacent piconets provide a bridge to support inner-piconet connections, allowing assemblies of linked piconets to form a physically extensible communication infrastructure known as Scatternet.

Spectrum

Bluetooth technology operates in the unlicensed industrial, scientific and medical (ISM) band at 2.4 to 2.485 GHZ, using a spread spectrum hopping, full-duplex signal at a nominal rate of 1600 hops/sec. the 2.4 GHZ ISM band is available and unlicensed in most countries.

Range

Bluetooth operating range depends on the device Class 3 radios have a range of up to 1 meter or 3 feet Class 2 radios are most commonly found in mobile devices have a range of 10 meters or 30 feet Class 1 radios are used primarily in industrial use cases have a range of 100 meters or 300 feet.

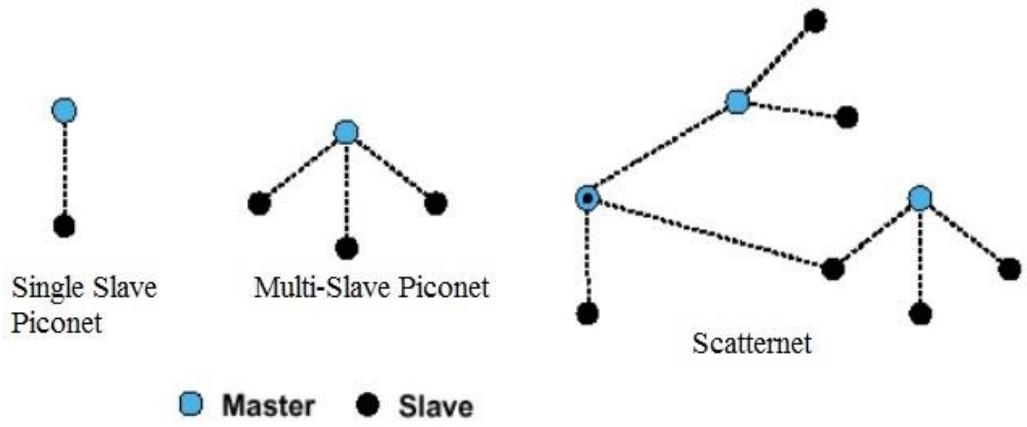
Data rate

Bluetooth supports 1Mbps data rate for version 1.2 and 3Mbps data rate for Version 2.0 combined with Error Data Rate.

Technical specifications or features and provides link to bluetooth physical layer,bluetooth MAC layer,bluetooth protocol stack,frequency allocations and bluetooth power classes.

Now-a-days bluetooth has become part of our lives due to its immense applications from audio devices which include headsets and mobile phones,home stereos,MP3 players, laptop,desktop,tablets and more. With bluetooth one can transfer data(meeting schedules,phone numbers), audio,graphic images and video from one device to the other provided they are bluetooth compliant. IEEE 802.15.1 standard describes detailed bluetooth specifications

Bluetooth Network




Bluetooth network consists of many bluetooth users. There are two types of network topologies in bluetooth viz. Piconet and scatternet. Piconet is formed by one master and one slave as well as one master and multiple slaves. There will be maximum 7 active slaves in the piconet. Hence there will be about 8 maximum devices communicating in a small network referred as piconet. Slaves can only transmit when they have been requested by the master bluetooth device. There will be about 255 slaves in parking state. Active slaves are polled by the master for transmission. Each station will get 8 bit parked address. Total 255 parked slaves are possible in one piconet. The parked station can join in just 2 ms. All the other stations can join in more time. About 10 such piconets exist in the bluetooth radio coverage area.

Combinations of multiple piconets is known as scatternet. A device can participate in multiple piconets. It will timeshare and need to be synchronized with the master of current piconet.

It supports data rate based on different versions from 720 kbps to about 24 Mbps. It will have distance coverage to about 1 to 100 meters based on power class supported on bluetooth devices.

Bluetooth technical specifications

Following are the technical features of bluetooth technology.

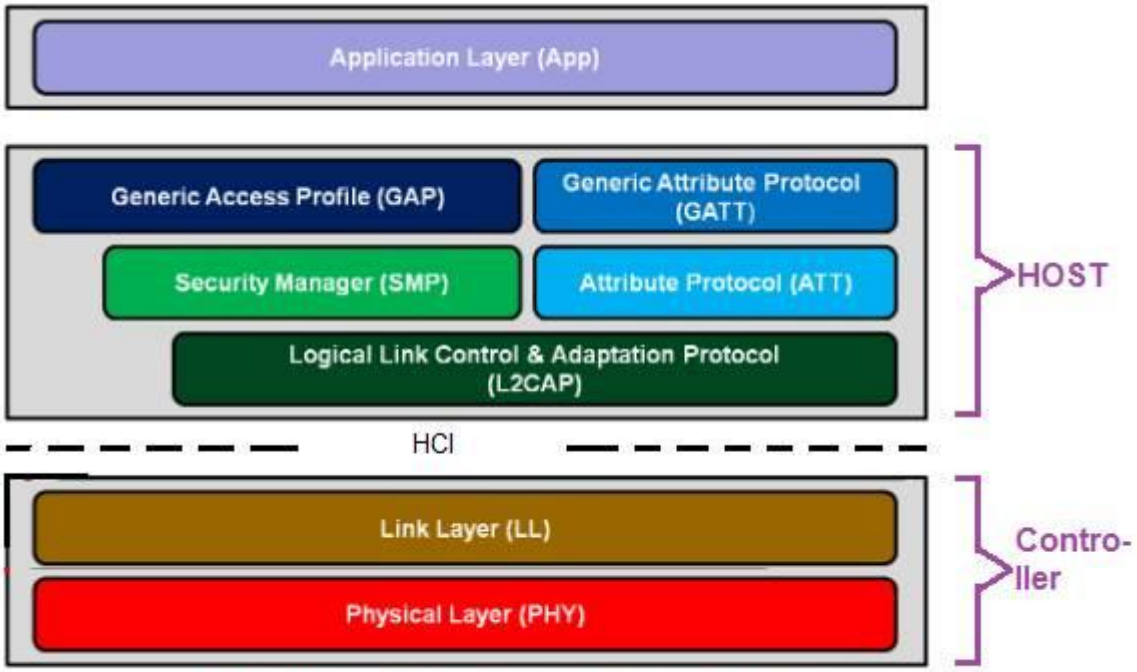
| Specification | feature supported |
|---|---|
| RF Frequency | 2.4GHz,READ MORE |
| Transmit power | 100 mW(Max.) 1mW(Min.),READ MORE |
| Data rate | About 1Mbps |
| Distance | 100 meter(max.), 1 meter(min.) |
| RF Bandwidth | 220 KHz to about 1MHz |
| Modulation type | Gaussian FSK (GFSK) |
| Number of RF carriers | 79(max.), 23(min.) |
| Topology | upto 7 links in a star configuration |
| hopping rate | 1600 hops per second |
| Access type | FH-TDD-TDMA |

## Bluetooth Applications

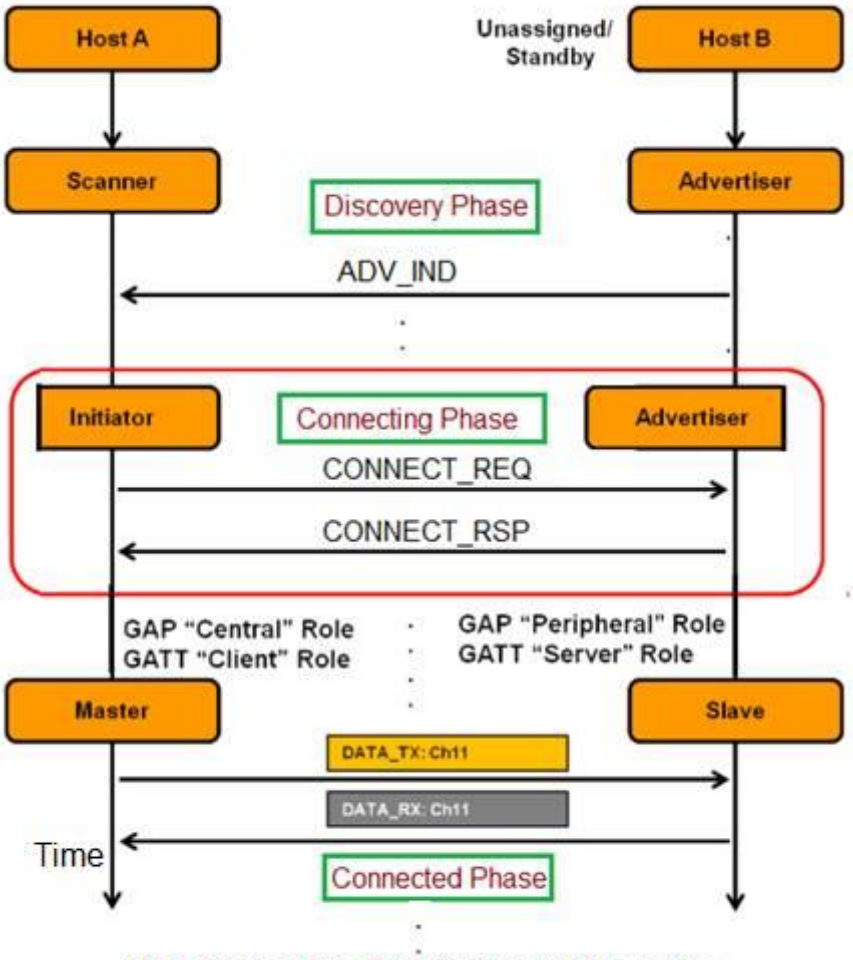
Following are few of the many bluetooth applications:

- One can receive and make call using bluetooth compliant wireless headset.
- Operate computer using mouse/keyboard and take print outs wirelessly eliminating cables.
- Home automation

BLE (Bluetooth Low Energy) Links




BLE (Bluetooth Low Energy) Protocol Stack




BLE Connection Establishment Procedure

**Bluetooth physical layer** consists of baseband and radio specifications as defined in IEEE 802.15.1.

Bluetooth network is composed of one master and one to seven slave devices. This small region is referred as piconet. Once master device selects channel with frequency hopping sequence and time to transmit, the same is used by other devices also in the same piconet. One bluetooth device of piconet can also exist and function as either master or slave in the other nearby biconet, this overlapping region is referred as scatternet.

**Frequency hopping**

It serves two purpose, one is that it helps provide resistance to multipath interference. Second one is that it provide multiple access to devices in different piconets co-located.

Bluetooth system uses frequency hopping scheme with about 80 different frequencies,with a carrier spacing of about 1MHz.With frequency hopping enabled, a logical channel is defined by hopping sequence. At any time 1 MHz bandwidth is shared by max. 8 devices. Different logical channels can utilize same 80 MHz BW at the same time. Collisions occur when two bluetooth devices use same hopping frequency simultaneously evenif they are on different piconets and different logical channels. The hopping rate is 1600 hops per second, hence physical channel exists for only 0.625ms.

Bluetooth radio uses TDD topology in which data transmission occur in one direction at one time and it alternates in two directions one after the other. The access is TDMA, as piconet medium is shared among two devices. Hence piconet access is referred as FH-TDD-TDMA.

**Physical links**

There are two ways link can be established between master and slave devices.

1. SCO referred as Synchronous connection oriented. In this type, fixed bandwidth is allocated for point to point connection between master and slave. The basic reservation is 2 consecutive slots. The master supports 3 SCO links and slave supports 2 or 3 links.

2. ACL referred as Asynchronous connectionless. This is used for point to multipoint link

between master and slaves. Only one ACL link exists and for more retransmission of packet is required. In the cases when slots are not reserved in SCO links, master device can exchange packets with any of the slave device on a per time slot.

**Baseband packet formats**

Bluetooth Packet Format = Access Code(72 bits) + Header(54 bits) + Payload (0 to 2745 bits)

Access code consists of preamble(4bits),sync word(64bits) and trailer field(4 bits).

Header field consists of AM_ADDR(3 bits), type(4 bits),flow(1 bit),ARQN(1 bit),SEQN(1 bit) and HEC(8 bits).

As mentioned above, access code in bluetooth packet is used for timing synchronization and other offset compensations. Access code is also used for paging requests, paging responses and inquiry purposes.

Header is used for identification of packet type and will carry protocol control information. Payload field will carry user voice or data. Channel Access code identifies a piconet, Device Access Code used for paging REQ/RES, Inquiry Access Code is used for inquiry purposes.

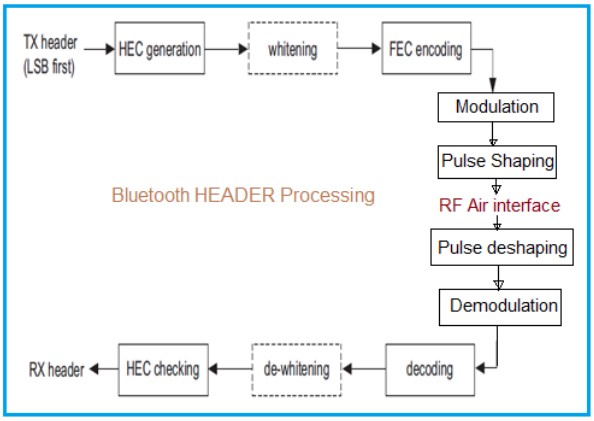
**Error Correction Methods**

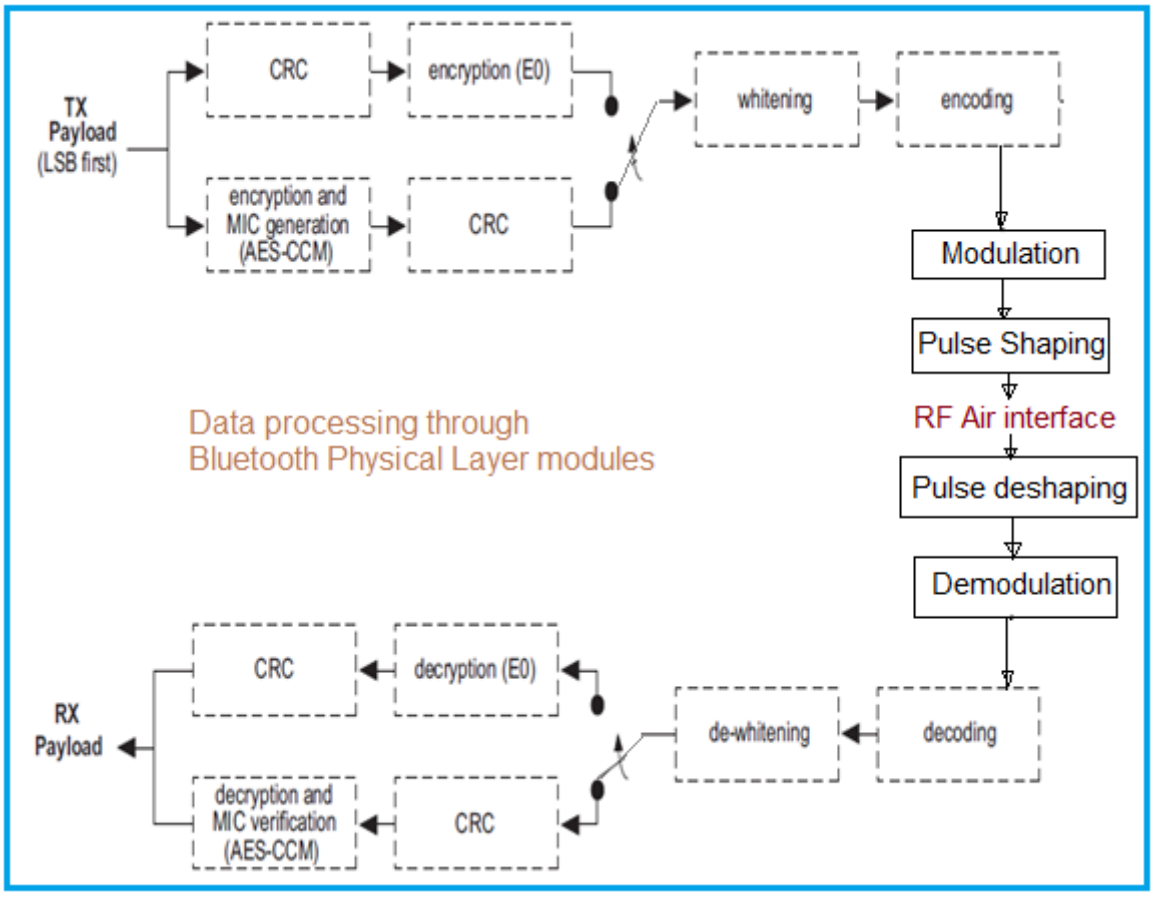
1/3 rate forward error correction (FEC)

2/3 rate forward error correction (FEC)

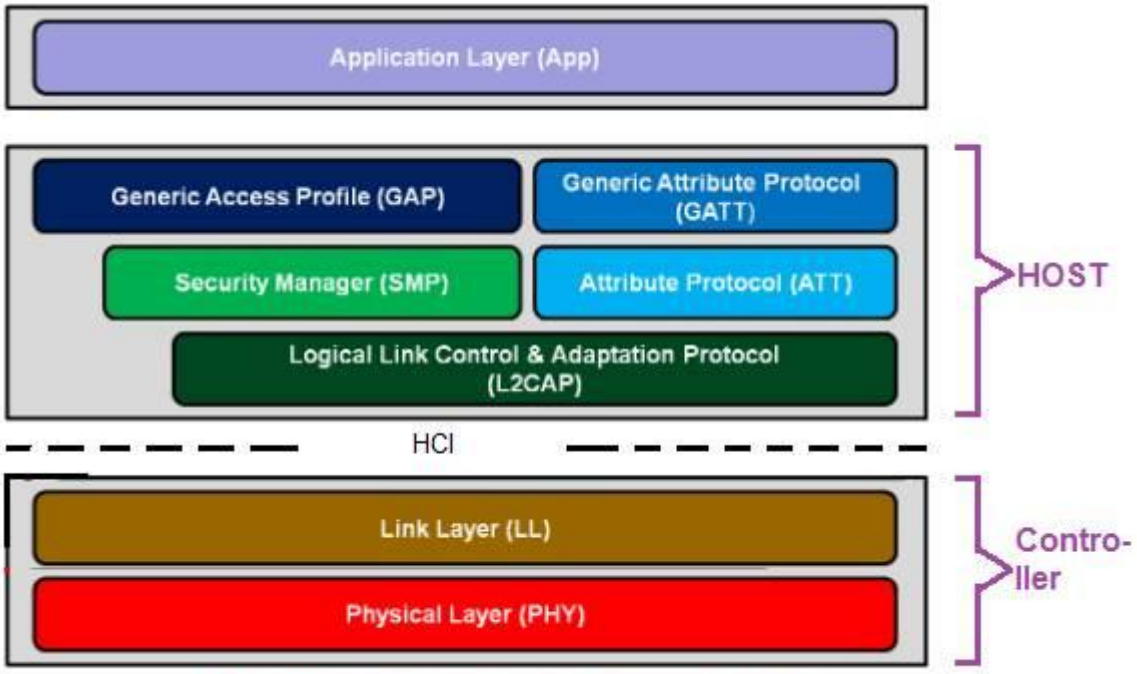
Automatic Repeat Request Scheme (ARQ)

**Header and payload processing through Bluetooth Physical layer➤**

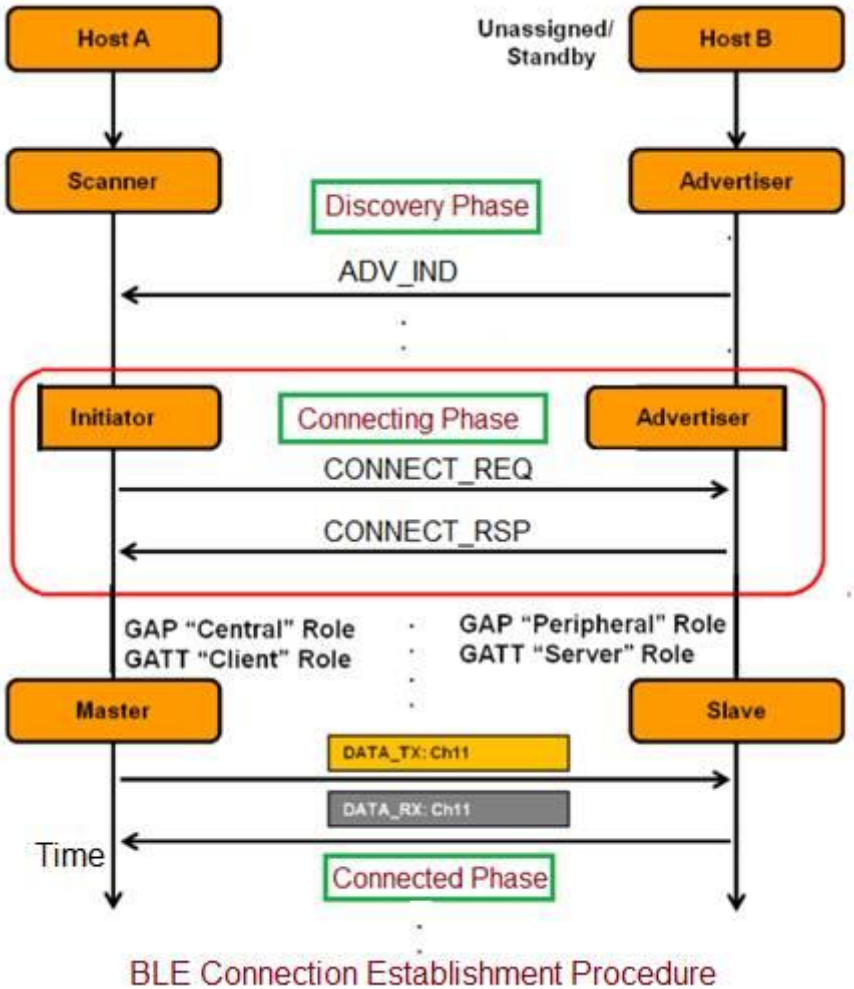


**BLE (Bluetooth Low Energy) Links**




BLE (Bluetooth Low Energy) Protocol Stack




BLE Connection Establishment Procedure

Bluetooth MAC layer consists of Link Manager Protocol(LMP) and Logical Link Control and Adaptation Protocol(L2CAP).

Logical channels

Bluetooth standard defines five different types of logical data channels based on different payload traffic carried by them. They are link control, link manager,user asynchronous,user isochronous and user synchronous. Link Control channel carry information such as ARQ,flow control and payload characterization.

Control Channels

Bluetooth modes of operation

During the connection state bluetooth device can be in one of the four modes which include active mode,sniff mode,hold mode and park mode.

In the Active mode, bluetooh device actively participates in the channel.

In the Sniff mode, bluetooth slave device will not listen on all the received slots but listen only specified slots for messages meant for it.

In the Hold mode, the bluetooth device does not transmit data for long time.

In the Park mode,the bluetooth device will have little activity to be performed and hence will consume very low power.

**Link Manager Protocol(LMP)**

LMP protocol is used to establish the link and to control the link. Link Control (LC) provides the reliability to Link Manager Protocol. LM PDUs are sent in single slot packets. PDU = Opcode(7bits), transaction ID(1bit), information contents

**Logical Link Control and Adaptation Protocol(L2CAP)**

This L2CAP protocol like LLC takes care of link layer protocol services between the entities. It provides services to upper layers and rely on lower layer for flow control as well as error control.L2CAP makes use of ACL links and does not use SCO links.

L2CAP provides two type of services connectionless and connection mode services. Connectionless type provide reliable datagram delivery service. Connection mode type provide service using HDLC protocol.

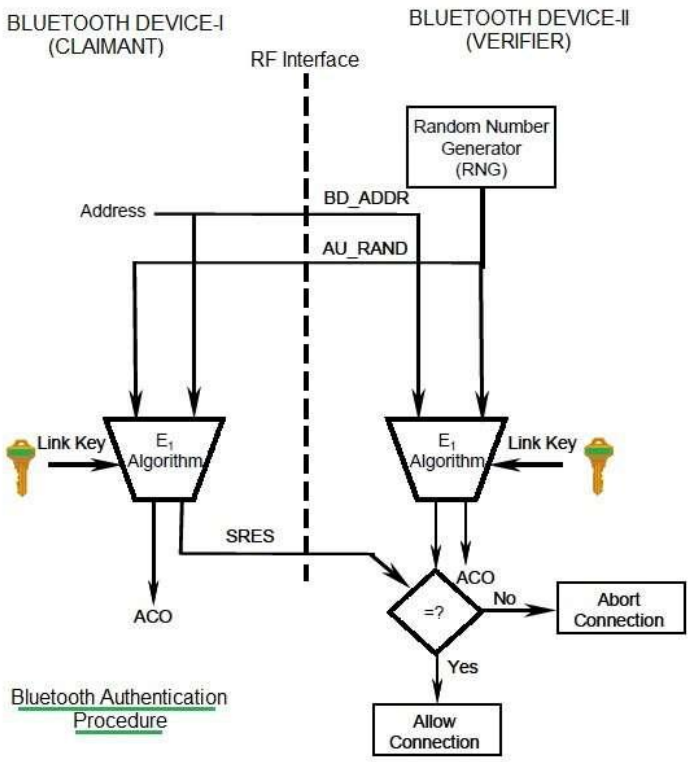
**bluetooth security** covers basics of security concepts in bluetooth network. There are three procedures in bluetooth viz. iniatialization, authentication and encryption.
Due to wide applications of bluetooth technology in our daily life, security of bluetooth devices have become a concern for the users. Though bluetooth devices are used in tandem with other WPAN devices but bluetooth security algorithms are developed to take care of authentication & encryption between only bluetooth devices on radio path(i.e. wireless).

The Bluetooth specification has defined three security services viz. authentication, confidentiality and authorization. Further bluetooth has three modes of security as follows.

SecurityMode1:Nonsecuremode
SecurityMode2:Servicelevelenforcedsecuritymode
Security Mode 3 : Link level enforced security mode

The **Bluetooth Link Key** is generated at the initialization phase. This phase occurs when two devices on bluetooth channel starts communicating or bonding. Both the associated devices derive link keys using the identical PIN entered in both of them by the user. After initialization procedure is completed the devices will perform authentication procedure and encryption procedure on the link. This is done automatically and transparently without any manual intervention of the user. Encryption key is derived from the link key generated.

**Authentication procedure for Bluetooth security**




Let us understand authentication procedure used as part of bluetooth security. Let us assume that bluetooth device-1 wants to access the bluetooth device-2 or want to pair the connection with it. Here device-1 is known as "claimant" and device-2 is known as "verifier".

• The device-1 transmits BD_ADDR(48-bit address) to device-2.
• The device-2 transmits AU_RAND(128-bit random challenge) to device-1.
• Both the device-1 and device-2 perform computations using E1-algorithm to calculate the SRES. E1 algorithms take BD_ADDR, AU_RAND and link key as inputs to calculate SRES.
• The device-1(claimant) returns the SRES in the response to device-2(verifier).
• The verifier does the comparison of returned SRES and the one it has calculated. SRES is of size32bits.
• If the SRES are equal, verifier will authenticate the claimant and allows connection establishment. Following are the useful fields and their sizes used in bluetooth authentication procedure. This procedure generates ACO field which will be used in bluetooth encryption procedure.

Device Address: 48 bits (Public Access)

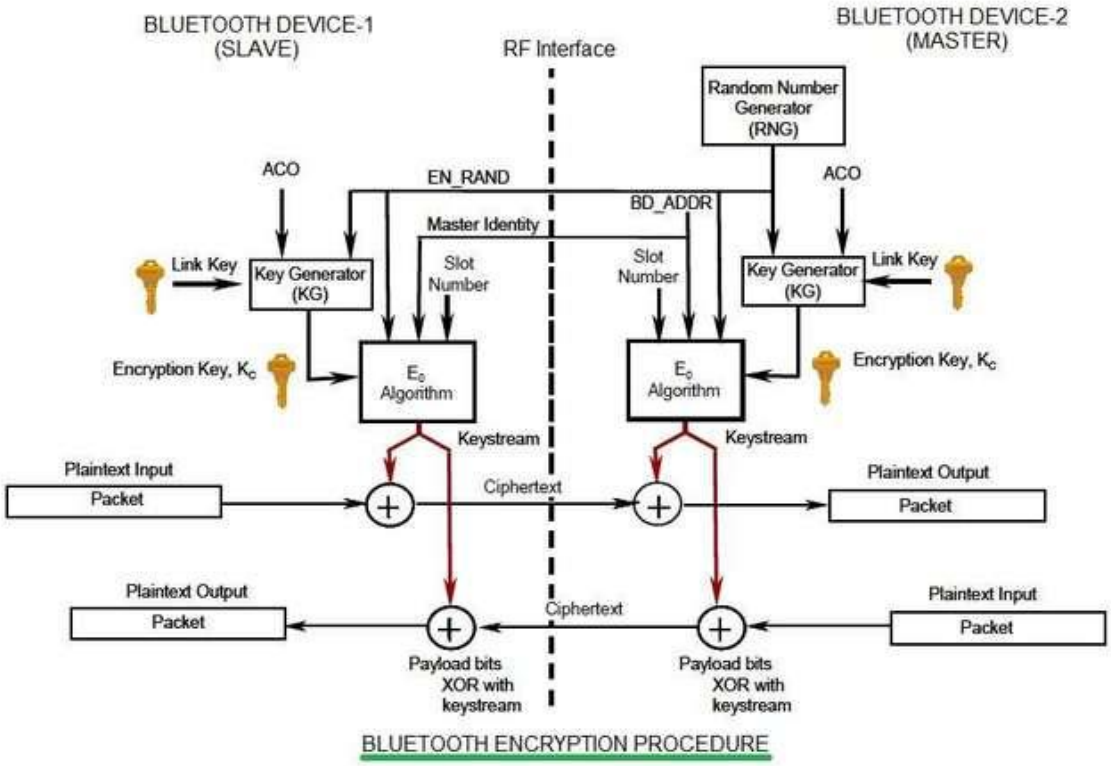
Random Challenge: 128 bits (Public, Unpredictable)

Authentication response('SRES'): 32 bits (Public)

Link Key: 128 bits (Secret)

ACO: 96 bit authenticated cipher offset

**Encryption procedure for Bluetooth security**




Bluetooth encryption is performed to protect payloads of the packet being exchanged between the two bluetooth devices. The encyption procedure in bluetooth security is based on E0 algorithm. Following steps are performed in the procedure:

• First using Key generator Encryption Key(Kc) is generated using inputs such as EN_RAND, ACO and Link Key.

• E0 algorithm uses EN_RAND, BD_ADDR, Slot number and encryption key(Kc) to generate 'Keystream'. • At last 'Keystream' generated is EX-OR[ed] with payload information bits. This('Ciphertext') is transmitted to the receiving device.

• The same steps are performed by the bluetooth device-2 for information transfer. This way 2-way bluetooth security is assured.

Following are the three encryption modes supported in bluetooth to provide confidentiality service.

• Mode1:Encryption is not performed on any type of traffic.

• Mode 2:Broadcast information is not encrypted while individually addressed information is encrypted using individual link keys.

• Mode 3:All the traffic informations are encrypted using master link key.

# UNIT-V

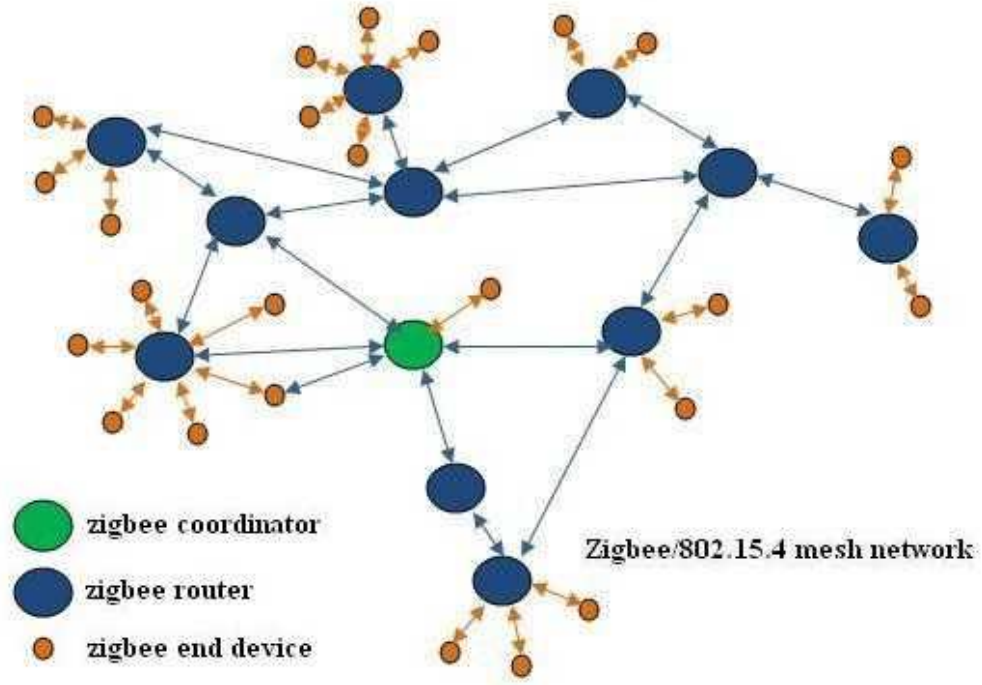
# THE IEEE 802.15 WORKING GROUP FOR WPANS

**Introduction**

Now-a-days zigbee is becoming very popular for low data rate wireless applications. Zigbee devices are used everywhere including smart energy, medical and in home automation. In smart energy applications zigbee products are used to monitor and control use of energy and water, which helps consumers save energy and water and save money too. In medical field it is used to connect unlimited number of health monitoring devices and many more. In home automation it controls domestic lighting, such as switches, dimmers, occupancy sensors and load controllers.

It has two bands of operation 868/915MHz and 2450MHz. 868/915 band provides about 20-40Kb/s and 2450MHz band provides about 250 kb/s data rates. In addition to this uses zigbee end devices can go to sleep mode which saves battery consumption and it also takes care of security of the information owing to security layer.

**Zigbee Network Overview:**



As mentioned in the network diagram, zigbee network is comprised of coordinator(C), router(R) and end devices (E). Zigbee supports mesh-routing. For detailed information on routing protocol employed in zigbee, one may refer Ad-hoc on-demand Distance Vector Routing protocol (AODV protocol), RFC 3561

**Coordinator**:

• Always first coordinator need to be installed for establishing zigbee network service, it starts a new PAN (Personal Area Network), once started other zigbee components viz. router(R) and End devices(E) can join the network(PAN).

• It is responsible for selecting the channel and PAN ID.

• It can assist in routing the data through the mesh network and allows join request from R and E.

• It is mains powered (AC) and support child devices.

• It will not go to sleep mode.

**Router**:

• First router needs to join the network then it can allow other R & E to join the PAN.

• It is mains powered (AC) and support child devices.

• It will not go to sleep mode.

**End Devices**:

• It cannot allow other devices to join the PAN nor can it assist in routing the data through the network.

• It is battery powered and do not support any child devices.

• This may sleep hence battery consumption can be minimized to great extent. There are two topologies, star and mesh, as mentioned Zigbee supports mesh routing. PAN ID is used to communicate between zigbee devices, it is 16 bit number. Coordinator will have PAN ID set to zero always and all other devices will receive a 16 bit address when they join PAN. There are two main steps in completing Zigbee Network Installation. Forming the network by Coordinator and joining the network by Routers and End devices.

**Forming the Zigbee Network**

• Coordinator searches for suitable RF channel which is usable and not interfering with Wireless LAN frequencies in use. This is because WLAN also operates in the same 2.4GHz bands.This is done on all the 16 channels. It is also referred as energy scan.

• Coordinator starts the network by assigning a PAN ID to the network. Assignment is done in two ways. Manual (pre configured) and dynamic (obtained by checking other PAN IDs of

networks already in the operation nearby so that PAN ID does not conflict with other networks). Here Coordinator also assigns network address to itself i.e. 0x0000.

• Now coordinator completes its configuration and is ready to accept network joining request queries from routers and end devices who wish to join the PAN.

• In addition to above, Coordinator(C) sends broadcast beacon request frame on remaining quiet channel. This is also referred as beacon scan or PAN scan. By this Coordinator receives PAN ID of routers(R) and end devices(E) present nearby. It also comes to know whether R/E allow join or not.

• Now R/E can join by sending association request to C. C will respond with association response.

**Joining the Zigbee Network**

• Let us examine how a router or end device joins zigbee network as part of zigbee tutorial. There are two ways to join a zigbee network viz. MAC association and network re-join.

• First one is implemented by device underlying MAC layer and second one is implemented by network layer, despite the name may also be used to join a network for the first time.

• MAC association can be performed between C and R/E or R and E or R and other R.

• Let us assume that Coordinator(C) has already established the PAN network. Hence next step for R or E is to find out whether C is allowing joining or not. So they do PAN scan or send beacon request frame.

• After they come to know that they can join the network, they will send association request frame and will join the network as soon as they receive the association response.

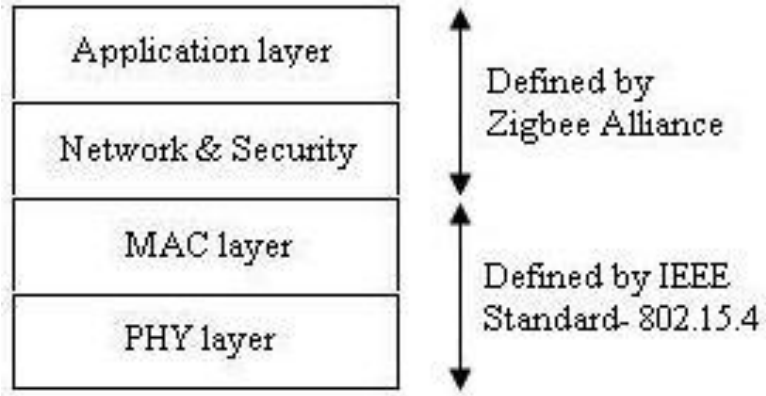
• As mentioned above whether or not C or R allow a new device to join depends on two main factors:

-Permit joining attribute

-Number of end device children it already has.

One of the applications of zigbee in home is that switch, speakers and lamp is controlled using zigbee technology.

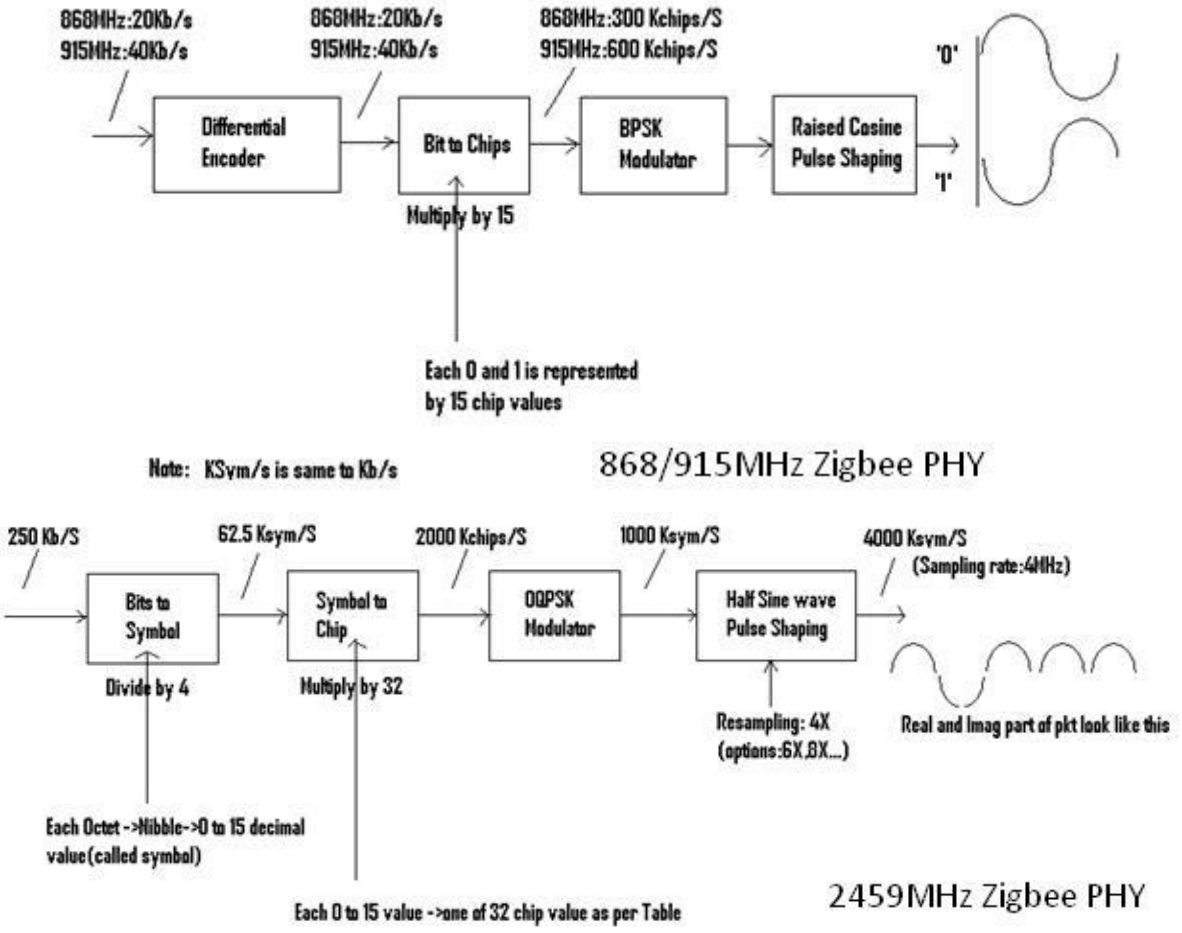
**zigbee protocol stack**




Zigbee Protocol Stack

zigbee IP consists of various protocol layers viz. physical layer(PHY), mac layer, network layer and application layer. IEEE 802.15.4 standard defined zigbee PHY and MAC specifications. Zigbee alliance specifies network and application layers.

**Zigbee Physical Layer**



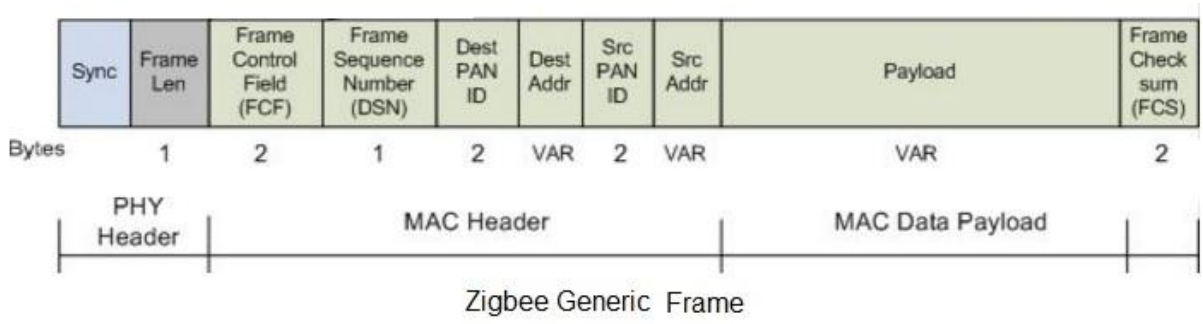
There are two physical layer version in zigbee. These are categorized based on frequency band of use viz. 868/915MHz and 2450MHz. The figure depicts the same. Refer Zigbee PHY for more information on working of physical layer and function of its modules.

**Zigbee MAC Layer**

| Octets:4 | 1 | 1 | | variable |
|---|---|---|---|---|
| Preamble | SFD | Frame length(7 bits) | reserved(1 bit) | PSDU |
| SHR | | PHR | | PHY payload |

Zigbee PHY Packet Structure

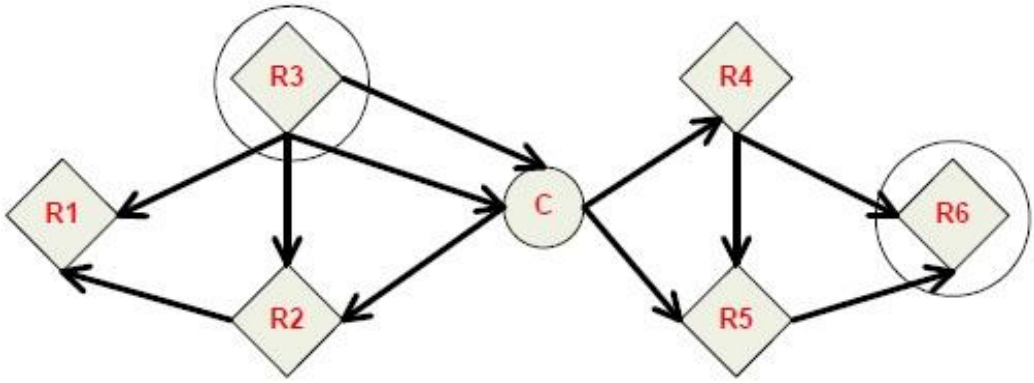
The figure depicts physical layer packet structure used to carry MAC frame of different types as per need.




Zigbee Generic Frame

Zigbee MAC frames include beacon, data, acknowledgment, MAC command and so on.

**Zigbee Network Layer**




Ad-hoc on-demand Distance Vector Routing protocol (AODV) is used at network layer.