Wireless LANs, 802.11

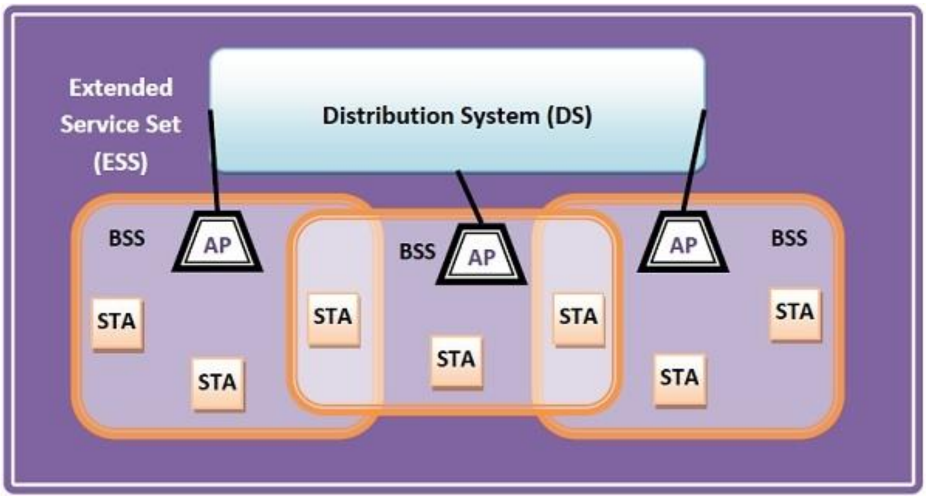
Wireless LANs (WLANs) are wireless computer networks that use high-frequency radio waves instead of cables for connecting the devices within a limited area forming LAN (Local Area Network). Users connected by wireless LANs can move around within this limited area such as home, school, campus, office building, railway platform, etc.

Most WLANs are based upon the standard IEEE 802.11 standard or WiFi.

Components of WLANs

The components of WLAN architecture as laid down in IEEE 802.11 are −

- **Stations (STA)** − Stations comprises of all devices and equipment that are connected to the wireless LAN. Each station has a wireless network interface controller. A station can be of two types −
  - Wireless Access Point (WAP or AP)
  - Client
- **Basic Service Set (BSS)** − A basic service set is a group of stations communicating at the physical layer level. BSS can be of two categories −
  - Infrastructure BSS
  - Independent BSS
- **Extended Service Set (ESS)** − It is a set of all connected BSS.
- **Distribution System (DS)** − It connects access points in ESS.



Types of WLANS

WLANs, as standardized by IEEE 802.11, operates in two basic modes, infrastructure, and ad hoc mode.

- **Infrastructure Mode** − Mobile devices or clients connect to an access point (AP) that in turn connects via a bridge to the LAN or Internet. The client transmits frames to other clients via the AP.
- **Ad Hoc Mode** − Clients transmit frames directly to each other in a peer-to-peer fashion.

Advantages of WLANs

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

Disadvantages of WLANs

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

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)

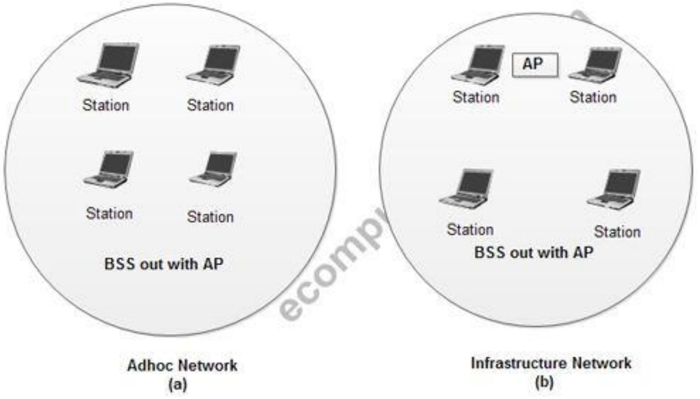
• The basic services set contain stationary or mobile wireless stations and a central base station called access point (AP).

• 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.

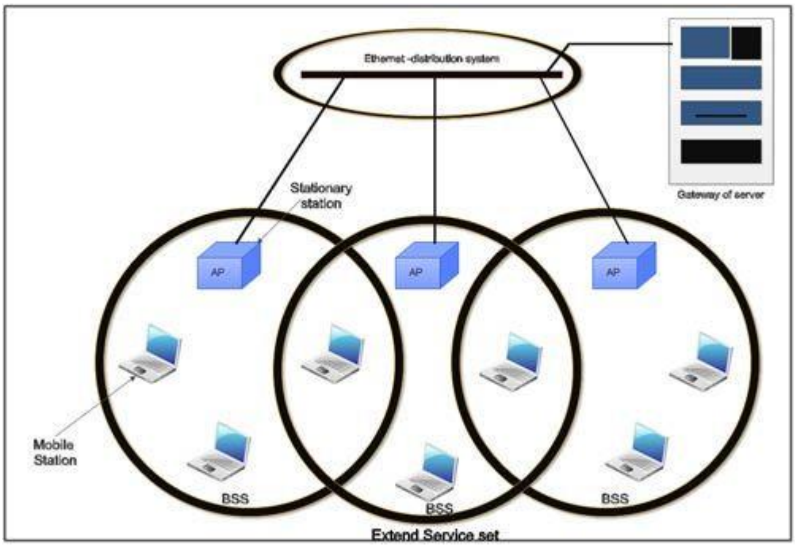
• The BSS in which an access point is present is known as an infrastructure network.



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).



Extend Service set

•

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

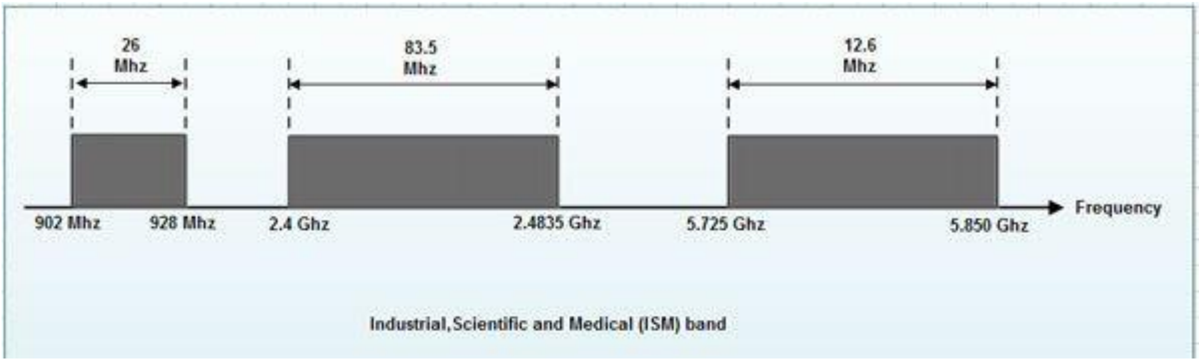
• As we know that physical layer is responsible for converting data stream into signals, the bits of 802.11 networks can be converted to radio waves or infrared waves.

• 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)

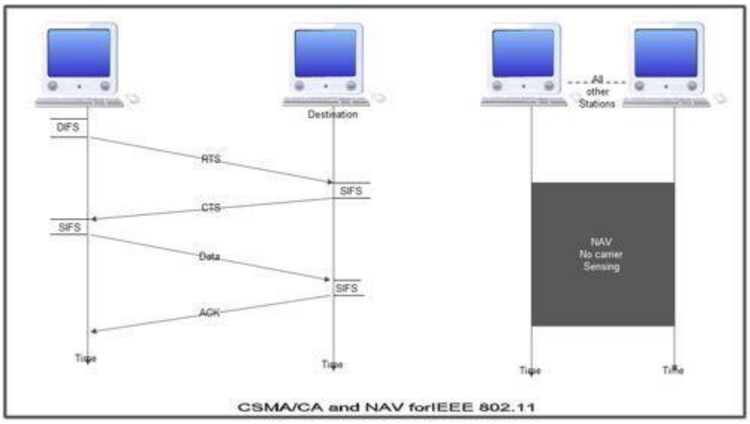
2. Point Coordination Function (PCF)

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.

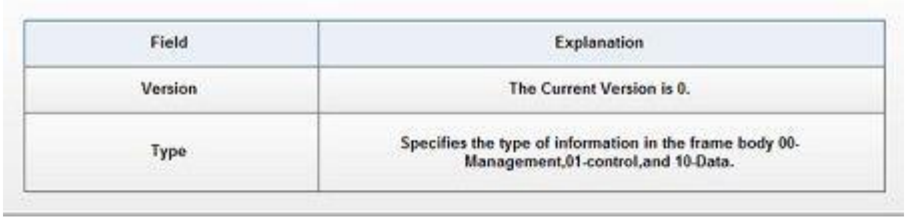
• When a station hears beacon frame, it start their NAV for the duration of the period of the repetition interval.

Frame Format of 802.11

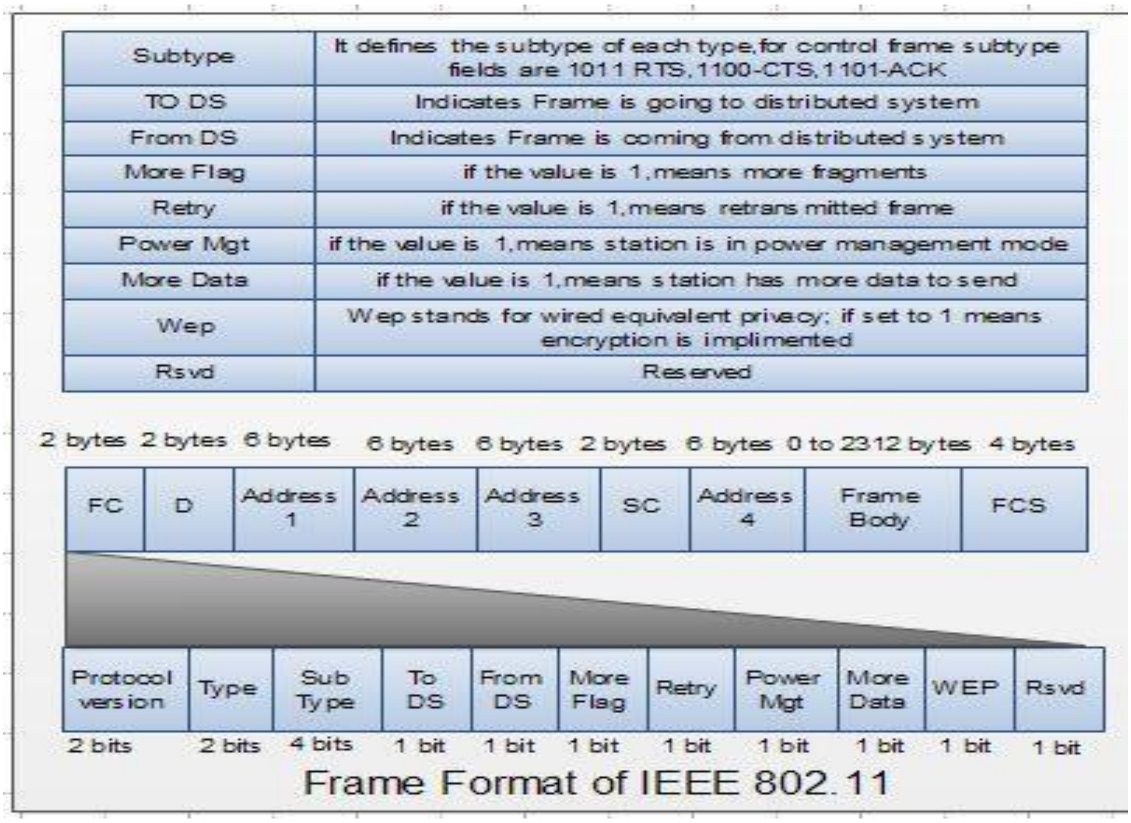
The MAC layer frame consists of nine fields.

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.



Subtype	It defines the subtype of each type,for control frame subtype fields are 1011 RTS,1100-CTS,1101-ACK
TO DS	Indicates Frame is going to distributed system
From DS	Indicates Frame is coming from distributed system
More Flag	if the value is 1,means more fragments
Retry	if the value is 1,means retransmitted frame
Power Mgt	if the value is 1,means station is in power management mode
More Data	if the value is 1,means station has more data to send
Wep	Wep stands for wired equivalent privacy; if set to 1 means encryption is implimented
Rsvd	Reserved

Frame Format of IEEE 802.11

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.

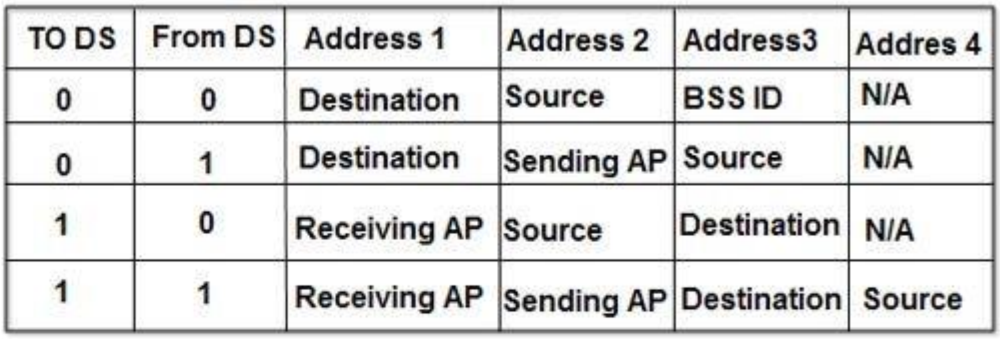
2. **Control frame**. These are used for accessing the channel and acknowledging frames. The control frames are RTS and CTS.

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.