- **Slot type (ST) :** This 1 bit field defines two types of slots, one for packet transmission and other for isochronous transmission.
- **Reserved (R) :** It is reserved for future.
- **Previous slot read (PSR) :** This two bit field is set to 0 by the addressed station once it has read the contents of the slot.
- **Request (RQ) :** It consists of three bits set by the station to make reservations for slot. These three bits represents 8 levels of priority in network.

2. **Address field :** The address field holds a 20 bit virtual channel identifier (VCI) to be used for MAN and WAN transmission.
3. **Type field :** This 2 byte field identifies the payload as user data, management data and so on.
4. **Priority field :** The priority field identifies the priority of slot in a network that uses priority.
5. **CRC field :** This field contains 8 bit CRC.

9.5 IEEE 802.11 : WIRELESS LAN

Wireless communication is one of the fastest growing technologies these days. Wireless LANs are commonly found in office buildings, college campuses, and in many public areas.

IEEE 802.11 standard provides wireless communication with the use of infrared or radiowaves.

802.11 Architecture

The 802.11 architecture 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 contains stationary or mobile wireless stations and a central base station called access point (AP).
- The use of access point is optional.

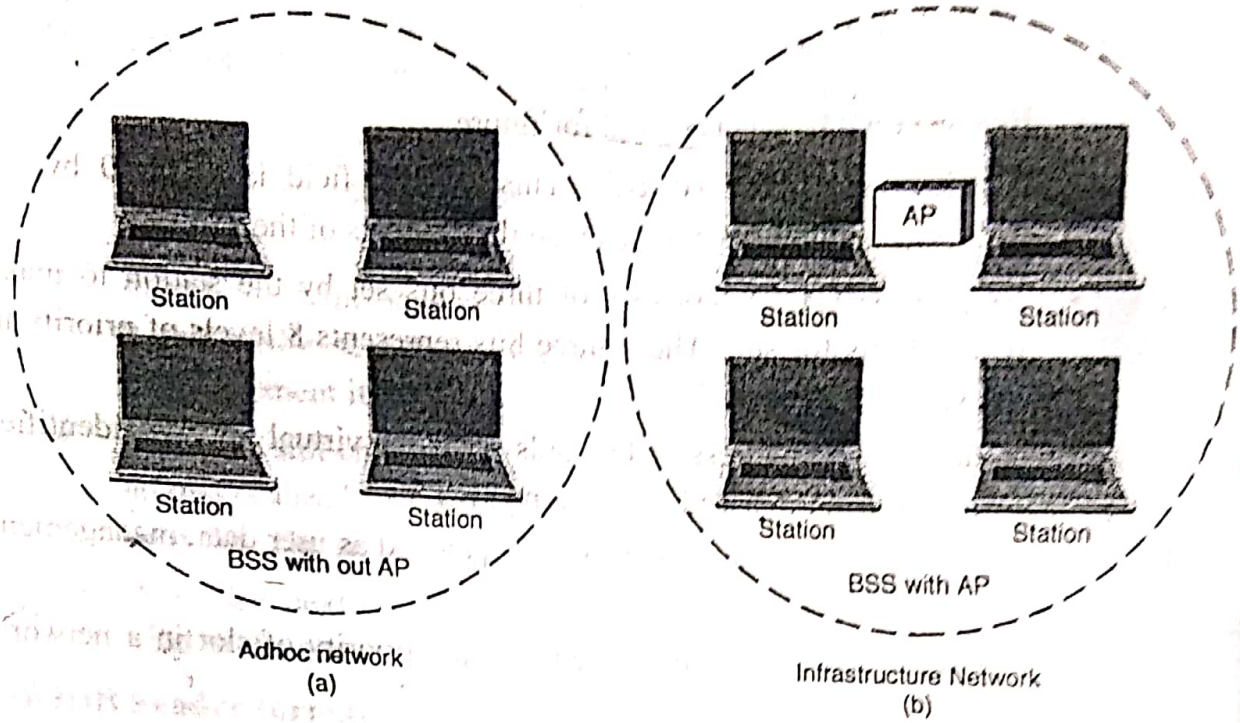

Fig. 9.56. Basic Service Sets

- 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** (see fig. 9.56 (a)).
- The BSS in which an access point is present is known as an **infrastructure network** (See fig. 9.56 (b)).

2. Extend Service Set (ESS)

- An extended service set is created by joining two or more basic service sets (BSS) having access points (APs) as shown in fig. 9.57.
- 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.

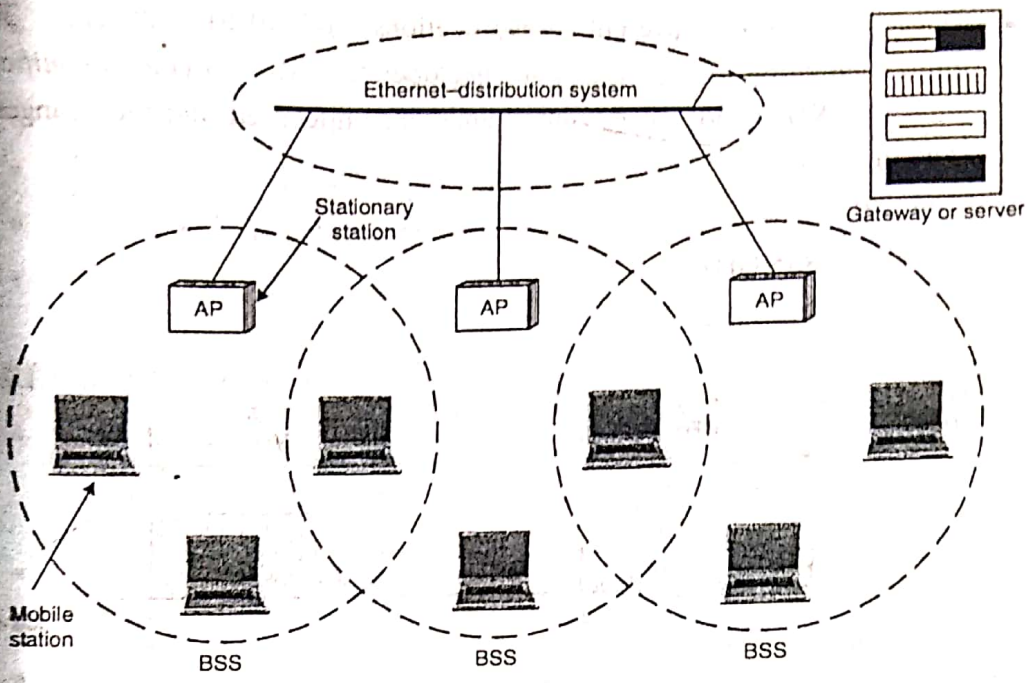

Fig. 9.57 Extended Service Set

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 type of stations can move from one BSS to another but the movement is limited inside an ESS.
3. **ESS-transition mobility :** These type of stations can move from one ESS to another. The communication may or 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 network can be converted to radio waves or infrared waves.

- These are six different specifications of IEEE 802.11. The implementations, except the first one, operates in *industrial, scientific and medical (ISM)* band. These three banks are unlicensed and their ranges are (See fig. 9.58)

  1. 902–928 MHz
  2. 2.400–4.835 GHz
  3. 5.725–5.850 GHz

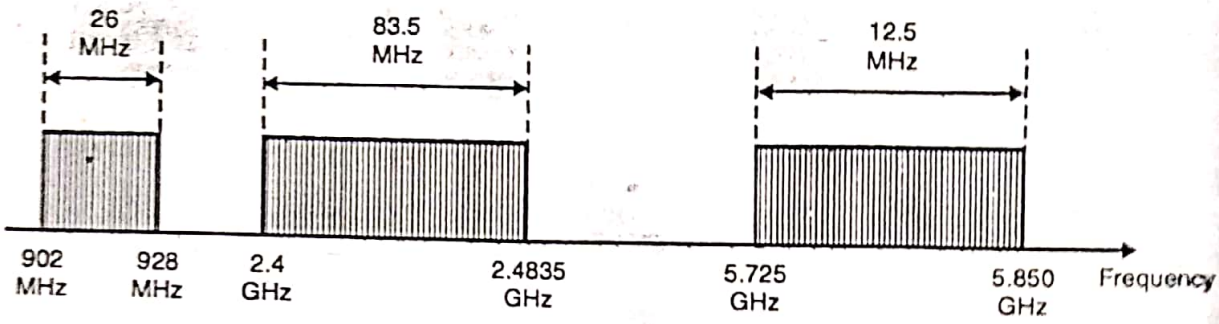

Fig. 9.58 Industrial, scientific and medical (ISM) band

- 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 : 1 Mbps and 2Mbps.
- For a 1-Mbps data rate, 4 bits of data are encoded into 16 bit code. This 16 bit code contains fifteen Os 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.* 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 Orthorgonal 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-DSSS

- 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 802.11b.

MAC sublayer Functions

802.11 supports 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 (see figure 9.59) :
  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.

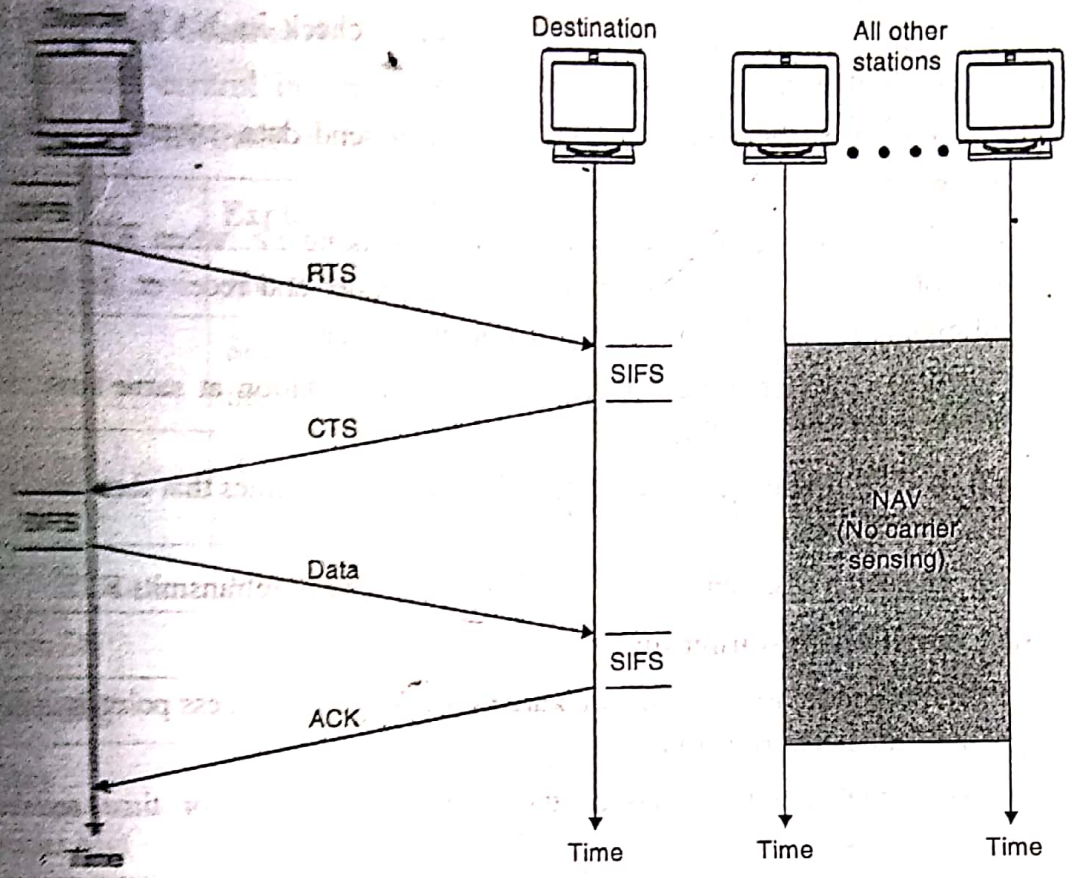

Fig. 9.59. CSMA/CA and NAV for IEEE 802.11

2. The sender then waits for SIFS time and sends data.
3. 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 called 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 NAV 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 as shown in fig 9.60.

Five Stages in the WiFi Network

WiFi client is going through the five stages:

1. Scanning
2. Joining
3. Authentication
4. Association
5. Reassociaton

Scanning

The scanning is the process of finding the WiFi network. Classical wired networks use cables for the interconnection. In the wireless network, the first thing you need to do is to to identify the appropriate network. WiFi **clients use the scanning to find existing networks in the area**. After scanning, the client can choose to join one of the available wireless networks.

Joining

Joining does not guarantee the network access. It is only the first step for the client to be connected to the WLAN network. After joining, the client also needs to pass the authentication and associate stage.

The client can connect to the BSS in two ways:

- Manually
- Automatically

In the manual joining the client chooses the BSS manually. In the automatic joining wireless client picks the best access point according to a power level and signal strength.
In the both cases, parameters configured on wireless client and access point, need to match.

Authentication

In wireless networks, you don't need the physical access to the network. You only need to be within the range. **Wireless authentication is the security method in the wireless networks**. More about the wireless authentication and authentication types read on wireless authentication.

Association

Association is the process that **enables the client the actual access to the WLAN network**. It is the same like plugging the cable into the wired network. It is not possible to be associated in more than one access point.

Reassociation

The association can occur only in the ESS wireless network. The client, in this case, associates to the other access point in the same ESS. It is triggered when the client detects that the other access point have a stronger wireless signal.

Comparison of Wi-Fi standards

As the Wi-Fi specification has evolved, its performance in terms of both range and throughput has improved, as the table below

Standard	802.11b	802.11a	802.11g	802.11n	802.11ac
Theoretical Speed – Up to	11 Mbps	54 Mbps	54 Mbps	300 Mbps	1 Gbps
Frequency	2.4 GHz	5 GHz	2.4 Ghz	2.4 and/or 5 Ghz	5 Ghz
Range ft	100 – 150	25-75	100 - 150	~ 230	Not known