MODULE III

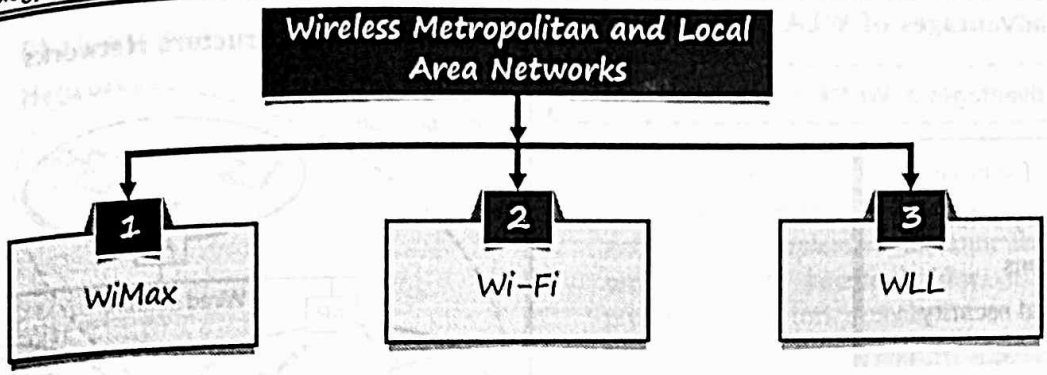
CHAPTER 3

Wireless Metropolitan and Local Area Networks

University Prescribed Syllabus w.e.f Academic Year 2021-2022

IEEE 802.16 (Wi-Max) – Mesh mode, Physical and MAC layer; IEEE 802.11(Wi-Fi) – Architecture, Protocol Stack, Enhancements and Applications.

Self-learning Topics : WLL(Wireless Local Loop).



3.1 INTRODUCTION

(For reading purpose only...)

- Wireless communication technologies support mobility, portability to the users. Hence it has gained immense popularity in day-to-day life nowadays.
- It has many advantages over wired communication. For example, wired networks rely on cables to connect digital devices together, wireless networks don't rely on wires or cables. This also reduces overall system cost. This also reduces errors due to cable damage.
- Wireless technologies are widely used in both home and business computer networks, for a variety of uses.

3.1.1 Types of Wireless Network Technologies

(For reading purpose only...)

A large number of technologies have been developed to support wireless networking in different scenarios.

(i) Bluetooth	(ii) WLAN
(iii) WMAN	(iv) MANET
(v) Wi-Fi	(vi) Wimax etc.

- Wireless local area network technologies comprise of fast growing flexible wireless access.
- This is generally useful in smaller organizations like offices, home, or production environments etc.
- WLAN is restricted to the distance parameters. They can be employed in limited ranges like in buildings, campus, single rooms etc.
- They are operated by individuals and not by the large-scale service providers.
- The main aim of WLAN technology is to remove the office cabling and provide the tether less access to internet. It also provides the flexibility to the ad hoc networks. For example, group meetings etc.

3.1.2 Advantages of WLAN

GQ. State advantages of WLAN.

1. Mobility
2. Low implementation cost
3. Installation speed and simplicity
4. Network expansion
5. Reliability
6. Scalability
7. Usage of ISM band

1. Mobility

Internet connectivity can be availed from any location.

2. Low implementation cost

WLANs are easy to set up, relocate, change and manage.

3. Installation speed and simplicity

The speed of installation is fast as no cabling is required. It also simplifies the architecture of the network.

4. Network expansion

Wireless technology reaches where cables cannot be reached.

5. Reliability

WLAN is resistant to different types of cable failures.

6. Scalability

WLAN can be configured in many topologies to meet the needs of the specific applications and installations.

7. Usage of ISM band

WLAN operates in the unlicensed ISM band available for use.

Modu 3

3.1.3 Disadvantages of WLAN

GQ. State disadvantages of WLAN.

1. Quality of service
2. Proprietary solutions
3. Restrictions
4. Safety and security

1. Quality of service

- WLAN offer lower quality of service as compared to wired LAN connection.
- This is due to lower bandwidth and limitations in radio transmission.
- WLAN also faces problems like higher data error rates due to interference, higher propagation delays.

2. Proprietary solutions

- Due to lack of standardization many companies are offering proprietary solutions.
- But these additional features work only when adapters from the same vendors are used.

3. Restrictions

- WLANs are limited to low power senders and certain license free frequency bands.
- These frequency bands may not be same worldwide. There is lack of government regulations.

4. Safety and security

Senders and receivers have to be controlled for low radiations.

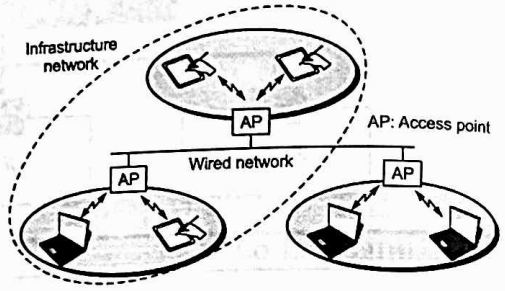
3.2 INFRASTRUCTURE AND AD HOC NETWORKS

GQ. Explain different network architectures of wireless networks.

WLANs have two different types.

1. Infrastructure networks
2. Ad hoc networks

3.2.1 Infrastructure Networks



(SD1)Fig. 3.2.1 : Infrastructure networks

- Refer Fig. 3.2.1. It shows an example of three infrastructure based wireless networks.
- Infrastructure based networks provides access to other networks, it includes forwarding functions, medium access control functions etc.
- In this communication takes place between wireless nodes and access points.
- Wireless nodes cannot directly communicate with each other.

Role of access point in infrastructure based WLAN

- It controls the medium access, and it acts as bridge between the existing wireless network and other wireless networks.
- Hence access points are used to connect several wireless networks to form one larger network beyond actual radio coverage.
- Most of the network functionality lies between the access point.
- Such type of network makes use of different access schemes with or without collision.
- There are chances of collision when the access point and the wireless nodes are not coordinated.
- But if only access point controls the medium access, then collision does not occur.
- This is important for better quality of service. Access point also polls the single wireless nodes to ensure the data rate.

3.2.1(A) Advantages of Infrastructure Networks

1. Simple design
2. When the access point takes full control of medium access, there are very less chances of collision.

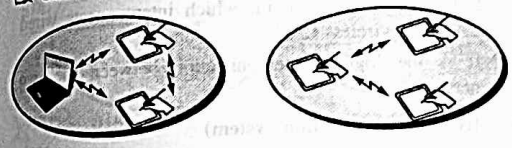
3.2.1(B) Disadvantage of Infrastructure Networks

1. These types of networks may lose flexibility of wireless networks. For example they cannot be used for disaster relief in case of no infrastructure is left.

Examples

1. Cellular networks
2. Satellite based cellular networks

3.2.2 Ad hoc Networks



(SD3)Fig. 3.2.2 : Ad hoc wireless networks

- These networks don't need any infrastructure to work.
- Each node can communicate directly with other nodes and access point is not needed in this.
- Refer Fig. 3.2.2 it shows an example of two ad hoc wireless networks with three nodes each.
- Nodes within ad hoc network can communicate only if they are in the coverage range of each other.
- They can also communicate if other nodes can forward their messages.
- In this the complexity of each node is higher as every node has to implement medium access mechanisms, mechanisms to handle hidden or exposed terminal problems and priority mechanisms.

3.2.2(A) Advantage of Adhoc Networks

1. This type of wireless network shows better flexibility.

3.2.2(B) Disadvantages of Adhoc Networks

1. Hardware complexity is main issue in ad hoc networks.
2. Two nodes can communicate only when they are in radio range of each other or other nodes are able to forward the data.

Examples

1. Third WLAN
2. Bluetooth

3.2.3 Comparison between infrastructure and ad hoc architectures of WLAN

GQ. Explain the difference between Ad-hoc Network and infrastructure based wireless networks.

Table 3.2.1 : Comparison between infrastructure and ad hoc architectures of WLAN

Sr. No.	Parameter	Infrastructure based Network	Ad hoc networks
1.	Working principle	Devices on this type of network all communicate through a single access point, which is generally the wireless router.	Ad-hoc networks don't require a centralized access point. Instead, devices on the wireless network connect directly to each other.
2.	Presence of access point	Required	No
3.	Limitation on range by	Wireless routers that acts as access points have higher-power wireless devices so they can cover a larger range	Wireless devices used are generally of low power. Hence range is limited.
4.	Communication with the receiver when it is not in range	If a receiver is out of range of sender, then forwarding of packets is done via access point.	If a receiver is out of range of sender, it will pass the data through other devices on the way.
5.	Hardware	Simple design of individual node	More complex design of individual node as compared to infrastructure based network.
6.	Flexibility	Less flexible	Higher flexibility
7.	Time required for setting up of network	More	Less
8.	Architectural diagram	Refer Fig. 3.2.1	Refer Fig. 3.2.2

3.3 IEEE 802.11 (WI-FI)

In the family of IEEE 802.11 many WLAN standards are included. The main goal of this standard is to set up simple and robust WLAN which offers time- bounded and asynchronous services.

Syllabus Topic : IEEE 802.11(Wi-Fi) – Architecture

3.3.1 System Architecture of IEEE 802.11

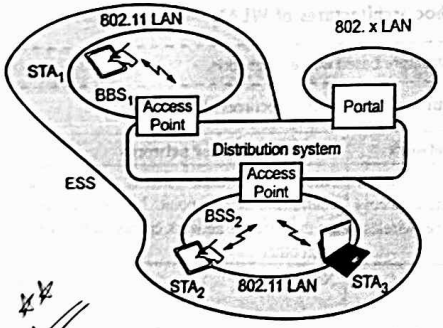
GQ. Explain different architectures of WLAN.

Wireless networks can exhibit two different basic system architectures.

A. Infrastructure based WLAN
B. Ad hoc WLAN

3.3.1(A) Infrastructure based WLAN Architecture

- Refer Fig. 3.3.1. It shows the system architecture of WLAN.



(5D2)**Fig. 3.3.1 : WLAN system architecture**

The system comprises of

(i) STA (Station)
(ii) Access Point (AP)
(iii) Portal (PO)
(iv) DS (Distribution System)
(v) BSS (Basic Service Set)
(vi) ESS (Extended Service Set)

(i) STA (Station)

It is nothing but a mobile station.

(ii) Access Point (AP)

- It is a special central traffic relay station that usually operates on fixed channel.
- It is stationary. It can be viewed as the coordinator in the group of stations.
- It is like the base station in GSM network.
- It supports roaming that is changing access points. They also control power management and synchronization functions.

(iii) Portal (PO)

- It is typical access point which interconnects wired LAN and wireless LAN.
- It is the logical interconnection between the two networks.

(iv) DS (Distribution System)

- DS is the backbone network that is responsible for the MAC layer transport of MAC service data units.
- Examples include 802.3 Ethernet, IEEE 802.4 token bus LAN, fiber optic LAN etc.
- A DS connects several BSSs via the AP to form a single network. Thus, it extends the wireless coverage area.
- It handles data transfer between the different APs.

(v) BSS (Basic Service Set)

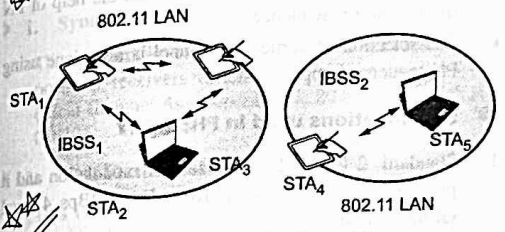
- It is the smallest building block of the WLAN system.
- It consists of some number of stations and access points in the network.
- Simplest BSS has only two STAs.
- The association of STA and BSS is entirely dynamic.
- BSS may be isolated, or it may be connected to the backbone Distribution System (DS) through an Access Point (AP).
- This mode of operation is known as ad hoc networking as this type of IEEE 802.11 WLAN is created and maintained without prior administrative arrangement.

(vi) ESS (Extended Service Set)

- It is a set of two or more BSSs forming a single sub-network.
- ESS configurations consist of multiple BSS cells that can be linked by either wired or wireless backbones known as DS.
- IEEE 802.11 supports ESS configurations in which multiple cells use the same channel.
- It may also use different channel to aggregate throughput.

- The STAs in ESS can be mobile or stationary.
- Stationary STAs are actually AP. They are part of wired LAN.
- When the BSSs are connected, two stations can communicate directly without AP.
- But if stations are belonging to different BSSs then they have to communicate via AP.

3.3.1(B) Ad hoc WLAN Architecture



(5D4)**Fig. 3.3.2 : ad-hoc WLAN architecture**

- Refer Fig. 3.3.2. It shows ad hoc WLAN architecture.
- In addition to infrastructure-based architectures, IEEE 802.11 also supports ad hoc network between stations.
- It forms IBSS (Independent Basic Service Set).

IBSS (Independent Basic Service Set)

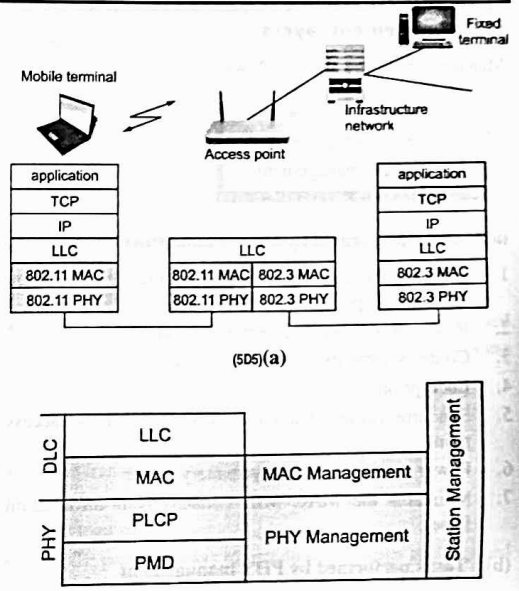
- When all the stations in BSS are mobile and it has no connection with other BSSs, the BSS is known as IBSS.
- It is an ad hoc network. This does not contain AP and it cannot transmit data to other stations.
- It is formed using one or more stations belonging to same radio frequency. The stations within the IBSS can communicate directly without APs.
- Several IBSS can be formed by keeping certain distance between them or by using different carrier frequencies.

Syllabus Topic : IEEE 802.11(Wi-Fi) -Protocol Stack, Enhancements and Applications

3.4 PROTOCOL ARCHITECTURE OF IEEE 802.11

GQ. Explain the protocol architecture of IEEE 802.11.

- Refer Figs. 3.4.1(a) and (b). Its shows the protocol architecture of IEEE 802.11 standard.
- As shown in the Fig. 3.4.1 (a), WLAN is connected to the IEEE 802.3 Ethernet vista bridge. WLAN behaves like slow wired LAN.



(5D5)(a)

(b)

(5D6)**Fig. 3.4.1: (a) and (b) protocol architecture of IEEE 802.11 standard**

- The higher layers (Application, TCP, IP) of wireless node works same as wired node.
- The upper part of data link control layer i.e. Logical Link Control (LLC) covers the differences of the medium access control layers needed for different media. IEEE 802.11 standard only covers the specification of physical layer and MAC layer.

Physical layer

- It is subdivided into Physical Layer Convergence Protocol (PLCP) and the Physical Medium Dependent sublayer (PMD) as shown in Fig. 3.4.1(b).
- PLCP sublayer provides a carrier sense signal. It is known as Clear Channel Assessment (CCA).
- It also provides common PHY Service Access Point (SAP). This SAP is independent of transmission technology used.
- The PMD sublayer handles the modulation and encoding/decoding of the signals.

MAC layer

Tasks performed are :

1. Medium access
2. Fragmentation of user data
3. Encryption

Management layers

Management layers are as follows -

(a) MAC management
(b) PHY management
(c) Station management

(a) Tasks performed by MAC Management

1. Supports the association and re-association of a station to an access point
2. Roaming between different access points
3. Controls authentication mechanisms
4. Encryption
5. Synchronization of a station with regard to an access point
6. Power management to save battery power
7. Maintains the MAC MIB (Management Information Base).

(b) Tasks performed by PHY management

1. Channel tuning.
2. Physical MIB (Management Information Base) Maintenance.

(c) Tasks performed by station management

1. Interaction with both management layers
2. Responsible for additional higher layer functions like control of bridging, interaction with distribution system in case of access point etc.

3.5 PHYSICAL LAYER

GQ. Explain the physical layer of IEEE 802.11.

- IEEE 802.11 supports three different physical layers.
  1. One layer based on infra red
  2. Two layers based on radio transmission
- All PHY variants has CCA provision. It is important in controlling MAC mechanisms and indicates if the medium is current idle.
- PHY layer offers an SAP with 1/2 MBPS transfer rate to the MAC layer.
- Four versions of PHY layer are

1. FHSS 2. DSSS
3. Infra-red 4. Narrowband microwave LANs

3.5.1 FHSS Frequency Hopping Spread Spectrum

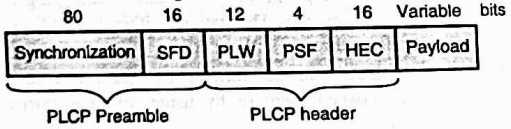
- FHSS is one of the variants of spread spectrum technology. It allows coexistence of multiple networks in the same area.
- It is done by separating different networks by different hopping sequences.
- Hopping sequences are generated with the help of PN (pseudo noise) sequence.
- The selection of particular channel is also done using PN sequence hopping pattern.

Specifications used in FHSS PHY

1. Standard 2 level GFSK is used for modulation and it provides transfer rate of 1MBps. For 2MBps 4 level GFSK is used.
2. It also uses the 2.4 GHz ISM band.
3. Provides bandwidth of 1 MHz.
4. Operation at 1 Mbit/s is mandatory while at 2 Mbit/s is optional.
5. 79 Hopping channels for North America and Europe and 23 hopping channels for Japan.
6. Maximum transmit power is 1 W/MHz in US, 100 mW EIRP in Europe and 10 mW/MHz in Japan.
7. FHSS is easier to implement

Frame structure used in FHSS PHY layer

- **Refer Fig. 3.5.1** it shows the format of IEEE 802.11 PHY frame using FHSS.



(SD7)**Fig. 3.5.1 : Format of IEEE 802.11 PHY frame using FHSS**

- The frame comprises of two parts
  1. PLCP part (preamble and header)
  2. Payload part
- PLCP part is always transmitted at 1 Mbps and payload which is MAC data may be transmitted at 2 Mbps.
- MAC data is scrambled using the polynomial $s(z) = z^7 + z^4 + 1$ for DC blocking and whitening of the spectrum.

Fields in the frame format

1. Synchronization
2. Start Frame Delimiter (SFD)
3. PLCP_PDU Length Word (PLW)
4. PLCP Signaling Field (PSF)
5. Header Error Check (HEC)

1. Synchronization

This pattern is used for the synchronization of the potential receivers and signal detection by the CCA (Clear Channel Assessment). It is 80 bit field which is a 010101.... Bit pattern.

2. Start Frame Delimiter (SFD)

This is a 16 bit field indicates the start of frame and provides frame synchronization. The pattern of SFD is 000011001011101.

3. Packet Length Word (PLW)

The 12 bit packet length width shows the length of the payload. The PLW can range between 0 to 4095.

4. PLCP Signalling Field (PSF)

It is 4 bit field that specifies the data rate of the payload following. If all bits are set to zero (0000) it means the lowest data rate (1 Mbit/s). 2 Mbit/s data rate is represented by 0010 bit sequence. Maximum data rate 8.5 Mbits/s is represented by 1111.

5. Header Error Check (HEC)

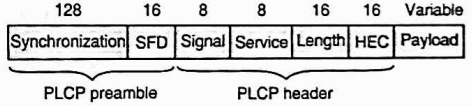
16 bit HFC is added to protect the PLCP header. It can recover errors of up to 2 bits, otherwise identify whether PLCP bits are corrupted.

3.5.2 Direct Sequence Spread Spectrum

- It is another spread spectrum technology used at Physical layer of IEEE 802.11.
- In this method spreading is achieved by code and not by frequency.
- In IEEE 802.11, 11 chip Barker code is used. It is (+1, –1, +1, +1, –1, +1, +1, +1, –1, –1, – 1).
- The main advantage of this technology is its robustness against interference and its insensitivity to multipath propagation.
- But the implementation is bit complex as compared to FHSS.

Specifications

- It also uses 2.4 GHz ISM band
- It offers both 1 Mbit/s and 2 Mbit/s data rate.
- It uses Differential Binary Phase Shift Keying (DBPSK) modulation for 1 Mbit/s transmission and Differential Quadrature Phase Shift Keying (DQPSK) for 2 Mbit/s.
- The symbol rate is 1 MHz and chipping rate is 11 MHz Implementation is complex.
- Provides a better coverage and a more stable signal
- All bits transmitted by the DSSS PHY are scrambled with the polynomial $s(z)=z^7+ z^4+1$ for DC blocking and whitening of the spectrum.
- Frame structure for IEEE 802.11 PHY using DSSS
- Refer Fig. 3.5.2.
- The frame consists of two parts
- PLCP part (preamble and header)
- Payload part
- PLCP part is always transmitted at 1MBps and payload which is MAC data may be transmitted at 2MBps.



(SD8)**Fig. 3.5.2 : Format of an IEEE 802.11 PHY Frame using DSSS**

Fields in the frame format

1. Synchronization 2. Start Frame Delimiter (SFD)
3. Signal 4. Service
5. Length 6. Header Error Check (HEC)

1. Synchronization

It is a 128 bit field is used for synchronization, gain setting, energy detection, and for frequency offset compensation. This field consists of scrambled 1 bits.

2. Start frame delimiter (SFD)

This field indicates the starting of a frame and consist the pattern 1111001110100000. This field is used for synchronization at the beginning of the frame.

3. Signal

This field indicates the data rate of the payload. The value 0x0A is for 1 Mbit/s and 0x14 is for 2 Mbits/s, other values are reserved for future use.

4. Service

This field is reserved for future use.

5. Length

This 16 bit field is used to indicate the length of a payload in microseconds.

6. Header Error Check (HEC)

HEC is used to protect PLCP header.

3.5.3 Infra-Red

- The PHY layer based on the infrared transmission, makes use of near visible light spectrum at 850-950mm.
- It does not need line of sight between the sender and the receiver. It also works with diffuse light.
- It supports point to multipoint communication.
- Maximum range is about 10m if no sunlight or heat sources interfere with the transmission.
- This is suitable for networks in buildings like classrooms, meeting rooms etc.
- Frequency reuse scheme implementation is very simple.
- A wall is more than enough to isolate one IR based IEEE 802.11 network from another. Infra red cannot penetrate through the walls or other opaque objects.
- Now a days this standard has been obsolete. No devices are available that offer infrared communication.

Advantages of Infra-red

1. Infrared can be more easily secured against eavesdropping as compared to microwave.
2. Separate infrared installation can be installed in every room in a building without interference enabling the construction of very large infrared LANs.
3. Equipment is relatively simple and inexpensive.

Disadvantages of Infra-red

1. Many indoor networks face the issue of intense infrared radiation from sunlight and indoor lighting. This ambient radiation appears as noise in an infrared receiver. Hence higher transmission power is needed.
2. Increment in transmission power has hazardous effects on eyes.

3.5.4 Narrowband Microwave LANs

- It makes use of narrowband microwave frequency for radio transmission. It is just wide enough to accommodate signal.
- It can make use of Licensed and Unlicensed (ISM) microwave bands for its operation.
- Microwave radio frequencies can be used for voice, data and video transmissions.
- They should be coordinated within certain geographic areas to avoid potential interference between the systems.
- In narrowband microwaves, cell configuration approach is employed. In these adjacent cells use non-overlapping frequencies within overall 18 GHz band.
- All transmissions are encrypted so that eavesdropping is avoided. This supports interference free communication.

Narrowband microwave LAN using unlicensed spectrum

- In 1995, Radio LAN has introduced narrowband wireless LAN using unlicensed ISM spectrum.
- It is used for transmission at low power of 0.5 watts or less.
- These Radio LAN products operates on 10 Mbps in the 5.8 MHz band.
- It has the range of 50 m in a semi-open office and 100 m in open office. It makes use of peer-to-peer configuration.
- The Radio LAN product automatically elects one node as the Dynamic Master based on parameters such as location, interference and signal strength.
- The identity of the master can change automatically as conditions change.
- The LAN also includes the dynamic relay function which allows each station to act as a repeater to move data between stations that are out of range of each other.

Note

Comparison of various Physical layer WLAN characteristics

GQ. Compare various physical layer WLAN characteristics.

Table 3.5.1 : Comparison of various Physical layer WLAN characteristics

Sr. No	Parameter	Infrared	FHSS	DSSS	Narrowband microwave
1	Data rate (Mbps)	Upto 10	1 to 3	2 to 54	10 to 20
2	Mobility	Stationary/ mobile	Mobile	Stationary/ mobile	Stationary/ mobile
3	Range (m)	Upto 25	30-100	30-250	10-40
4	Detectability	Negligible	Little	Little	Some
5	Wavelength / frequency	1:800 to900 nm	902-928MHz 2.4-2.4835GHz 5.725-5.85GHz	902-928 MHz 2.4-2.4835 GHz 5.725-5.85 GHz	902-928 MHz 4.9-5.775 GHz 18.825-19.205 GHz
6	Modulation used	ASK	GFSK	QPSK	FS/QPSK
7	Radiated power	--	61 W	61 W	25 mW
8	Access method used	CSMA	CSMA	CSMA	Reservation ALOHA, CSMA

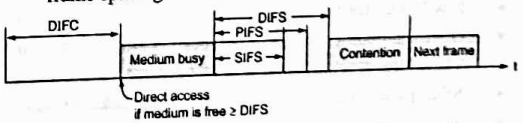
3.6 MEDIUM ACCESS CONTROL LAYER

GQ. Explain in Detail IEEE 802.11 MAC sublayer.

- The tasks performed by the MAC layers are
  1. Control medium access
  2. Supports roaming
  3. Authentication
  4. Power saving mechanisms
- The basic services provided by MAC layer are
  1. Asynchronous data service (mandatory)
  2. Time bounded service (optional)
- Asynchronous services support broadcast and multicast packets. Packet exchange is based on a best effort model which means no delay bounds can be given for transmission.
- IEEE 802.11 ad hoc network architecture offers only asynchronous data service however 802.11 infrastructure-based architecture offers both the services.
- There are three basic access mechanisms defined for IEEE 802.11, they are
  1. Method based on CSMA/CA (mandatory)
  2. Method to avoid hidden terminal problem
  3. Contention free polling method for time bound service
- Method based on CSMA/CA (mandatory) and Method to avoid hidden terminal problem are also known as Distributed Coordination Function (DCF) and Contention free polling method for time bound service is also known as Point Coordination Function (PCF).
- DCF offers only asynchronous service whereas PCF offers both asynchronous and time bounded services. PCF needs access point to control medium access and to avoid contention.
- MAC mechanisms are also known as Distributed Foundation Wireless Medium Access Control (DFWMAC).

Parameters for controlling the waiting time before medium access

- There are three different parameters that define the priorities of medium access.
- The values of the parameters depend on the PHY and are defined in relation to a Slot time.
- Slot time is described based on medium propagation delay, transmitter delay and other PHY dependant parameters. Slot time is 50μs for FHSS and 20μs for DSSS.
- CCA detects whether the medium is busy or idle. If the medium is busy may be due to data frames or other control frames. During the contention phase several nodes try to access the medium.
- Refer Fig. 3.6.1. It shows medium access and inter-frame spacing.



(509) **Fig. 3.6.1 : Medium access and inter-frame spacing**

- The parameters are :
  1. Short Inter Frame Spacing (SIFS)
  2. PCF Inter Frame Spacing (PIFS)
  3. DCF Inter Frame Spacing (DIFS)

1. Short Inter Frame Spacing (SIFS)

- It has the highest priority.
- The shortest waiting time for medium access is defined for short control messages like acknowledgements of data packets or polling responses.
- The SIFS for DSSS is 10µs and for FHSS it is 28µs.

2. PCF Inter Frame Spacing (PIFS)

- It has medium priority.
- A waiting time between DIFS and SIFS is used for a time bounded service. PIFS is defined as SIFS plus one slot time.
- An access point polling other nodes only has to wait PIFS for medium access.

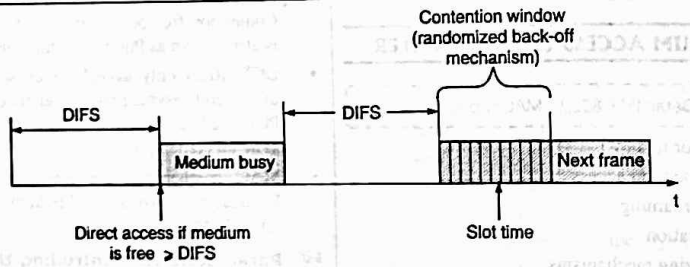
3. DCF Inter Frame Spacing (DIFS)

- It has lowest priority.
- It has the longest waiting time. This is used for asynchronous data service within a contention period. It is defined as SIFS plus two slot times.

3.6.1 Basic DFWMAC-DCF using CSMA/CA

GQ. Explain Basic DFWMAC-DCF using CSMA/CA.

- The mandatory access mechanism of IEEE 802.11 is based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).
- It is random access scheme with carrier sense and collision avoidance through random backoff.
- **Refer Fig. 3.6.2.** It shows basic CSMA/CA mechanism.



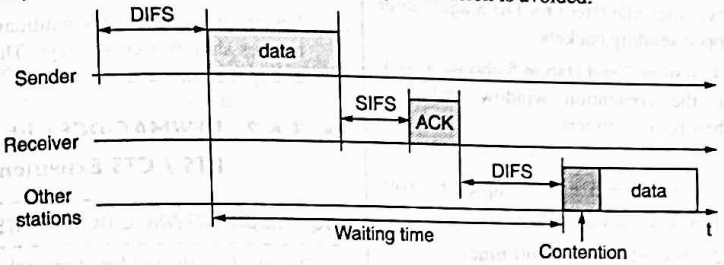
(5D10)**Fig. 3.6.2 : Basic CSMA/CA mechanism**

Working of Basic DFWMAC-DCF using CSMA/CA

- A node can access the medium at once if the medium is idle for the duration of DIFS. It supports short access delay under light load. Additional mechanisms are needed if large number of nodes are needed to access the medium.
- If the medium is busy, nodes must wait for DIFS duration before entering the contention phase.
- Each node chooses a random backoff time within a contention window. It delays medium access for this random amount of time.
- Node keeps on sensing the medium. Once node senses that channel is busy, it has lost this cycle and has to wait for the next chance. If the randomized additional waiting time is over for a node and if the medium is still idle, the node can access medium immediately.
- Basic CSMA/CA is not fair. Hence IEEE 802.11 adds a backoff timer to provide fairness.
- Each node selects the random waiting time within the range of the contention window.
- If one of the stations does not get access to medium in first cycle, it will stop its backoff timer.
- It will wait for the channel to be idle again for DIFS and starts the counter again.
- Once the counter expires, the node accesses the medium.
- Therefore, deferred stations don't choose a randomized backoff time again, rather they continue to count down.
- Stations will have to wait only for their backoff timer from the previous cycle.
- This is the advantage in case of the stations which are waiting for longer time as compared to the stations that are entered recently.

Unicast data transfer

- **Refer Fig. 3.6.3.** It shows the sender accessing the medium and sending its data.
- In this receiver answers directly by Acknowledgement (ACK). The receiver waits for SIFS duration and then accesses the medium.
- During this interval, no other station can access the medium, so collision is avoided.

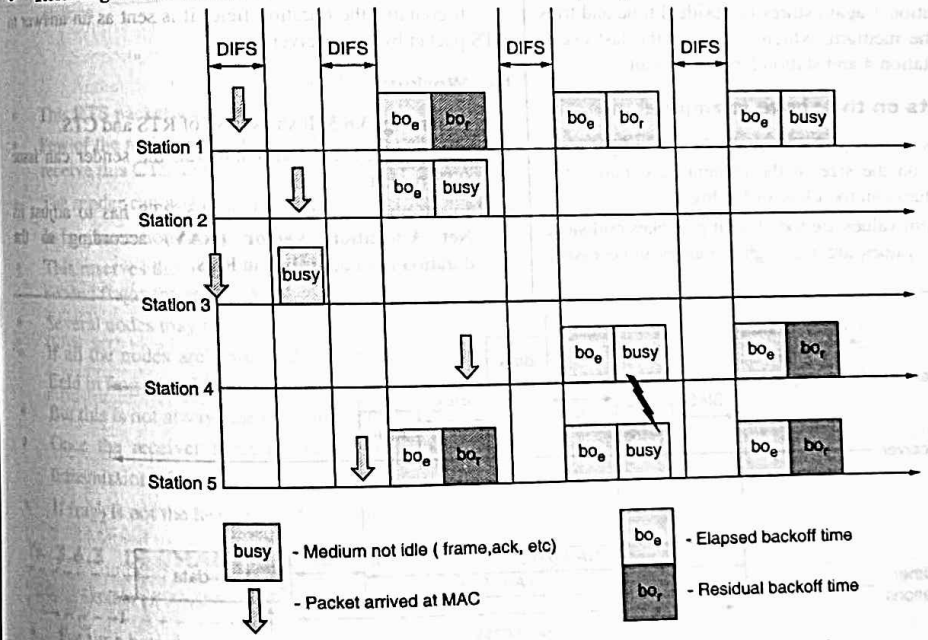


(5D11)**Fig 3.6.3 : IEEE 802.11 Unicast data transfer**

- Other stations need to wait for DIFS plus their backoff time interval to get the access.
- Acknowledgement from the receiver assures the correct reception of frame on the MAC layer. This is important in error prone environments like wireless links.
- If the sender does not get ACK from the receiver, it automatically retransmits the frame. After that sender has to wait for its turn to access the medium. The number of retransmissions is limited, and final failure is reported to the higher layers.

Example of basic DFWMAC-DCF with several senders

- **Refer Fig. 3.6.4.** It shows basic DFWMAC-DCF with five competing senders.



(5D12)**Fig. 3.6.4 : Basic DFWMAC-DCF with several competing senders**

Let station 3 has the first request from the higher layer to send a packet.

- **Step 1 :** Station 3 senses the medium, waits for DIFS and starts sending packets using medium.
- **Step 2 :** Station 1, station 2 and station 5 needs to wait till the medium becomes idle (free) for DIFS again after station 3 has stopped sending packets.
- **Step 3 :** Station 1, station 2 and station 5 choose a back off time within the contention window and start counting down their backoff timers.

Backoff times

1. For station 1and station 5 = bo_e (elapsed backoff time) + bo_r (residual backoff time)
2. For station 2 = bo_e (elapsed backoff time)

- **Step 4 :** After completion of the backoff time of station 2, it gets the medium access.
- **Step 5 :** Now if station 4 also wants to send packets, after DIFS wait time, three stations namely station 1, station 5, and station4 tries to access the medium.

- As shown in Fig. 3.6.4 the backoff time of station 4 and station 5 is same hence both of them can access the medium at the same time. This results in collision. Hence the transmitted packets are lost. This collision triggers retransmissions with new random backoff time.

- **Step 6 :** Station 1 again stores its residual time and tries to access the medium, which is gets in the last cycle. This time station 4 and station 5 needs to wait.

☞ Comments on the above example

1. Access scheme has problems under heavy or light load. Depending on the size of the contention window, the random values can too close or too high.
2. If the random values are too close it provokes collision. And if the values are too high it causes unnecessary delay.
3. The contention window doubles up to maximum each time the collision occurs.
4. The larger the contention window, the greater is the resolution power of the randomized scheme. There is less probability of choosing the same random backoff time value if the contention window is large.
5. Under the light load conditions, contention window assures shorter access delays. This algorithm is known as exponential backoff.

3.6.2 DFWMAC-DCF with RTS / CTS Extension

GQ. Explain DFWMAC-DCF with RTS / CTS extension.

To deal with hidden terminal problems RTS/CTS protocols are defined in IEEE 802.11.

RTS (request to send)

- It is a control packet. This packet is not given any higher priority compared to other packets.
- It includes the receiver of the data transmission and the duration required for the data transmission including packet transmission and ACK reception.

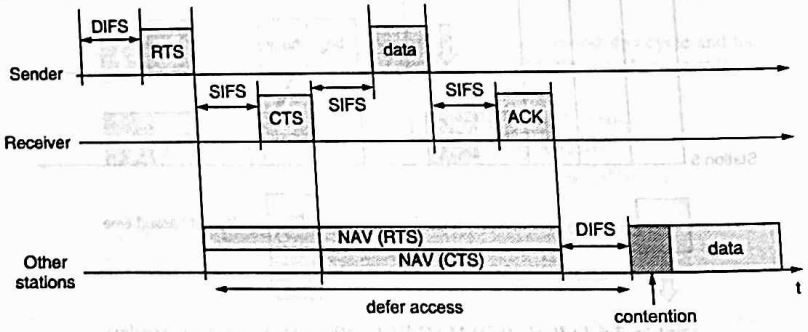
CTS (clear to send)

It contains the duration field. It is sent as an answer to RTS packet by the receiver.

☞ Working

Refer Fig. 3.6.5. It shows use of RTS and CTS.

- After waiting for DIFS interval, the sender can issue RTS packet.
- Every node which receives the RTS has to adjust its **Net Allocation Vector (NAV)** according to the duration field described in RTS.



(5D13)**Fig. 3.6.5 : IEEE 802.11 hidden node provisions for contention-free access**

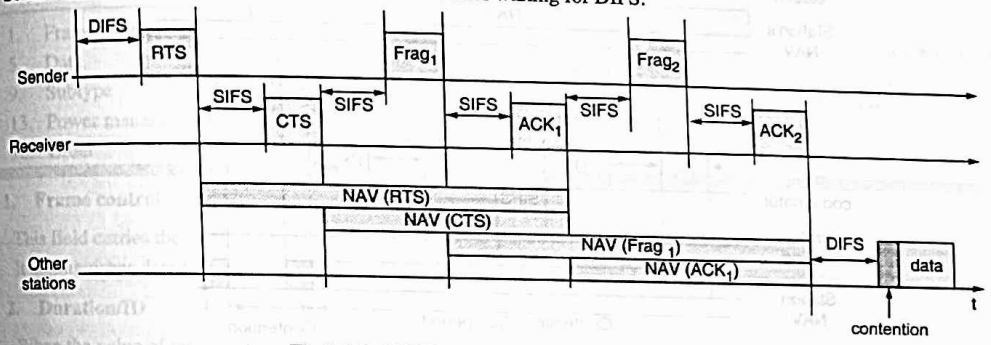
- NAV specifies the earliest point at which the station can try access the medium.
- On reception of RTS. Receiver answers with CTS after waiting for SIFS interval.
- All the stations receiving CTS, must adjust their NAV according to the duration specified in CTS.
- All the stations in the receiving distance of sender and receiver are informed that they have to wait for more time before accessing the medium.
- This reserves the medium for single sender. Hence it is also known as virtual reservation scheme.
- After completion of SIFS duration, sender can send the data. Receivers send the ACK after SIFS waiting time.
- Once the transmission is completed, the NAV in each node marks the medium as free and standard cycle starts again.

☞ Disadvantage of RTS/CTS scheme

It causes non-negligible overhead which results in bandwidth wastage and higher delay.

☞ Fragmentation of user data

- **Refer Fig. 3.6.6.** It shows mechanism for fragmentation of user data.
- Sender sends the RTS packet to reserve the medium after waiting for DIFS.



(5D14)**Fig 3.6.6 : IEEE 802.11 fragmentation of user data**

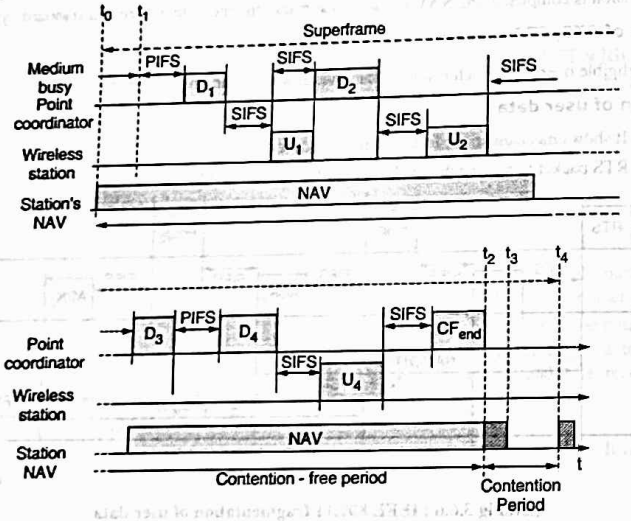
- This RTS packet includes the duration for the transmission of the first fragment and the corresponding ACK.
- Few of the nodes which receive this RTS can adjust their NAV accordingly. Receiver answers with CTS. Few receivers receive this CTS and they adjust their NAV accordingly.
- The sender can now send first data frame $frag_1$ after waiting for SIFS interval.
- In fragmentation mode, another duration value is included in $frag_1$.
- This reserves the medium for the said duration of the transmission following. This following transmission comprises of second fragment and its ACK.
- Several nodes may receive this reservation and set their NAV accordingly.
- If all the nodes are static and transmission conditions have not changed, then the set of nodes receiving the duration field in $frag_1$ should be same as the set of nodes that has received the initial RTS.
- But this is not always the case due to mobility in the network.
- Once the receiver receives $frag_1$ it answers with ACK after SIFS interval including the reservation for the next transmission of $frag_2$.
- If $frag_2$ is not the last frame of transmission, process continues.

3.6.3 DFWMAC-PCF with Polling

GQ. Explain DFWMAC-PCF with Polling.

- For time bounded service, the standard PCF (Point Coordination Function) is specified on the top of the standard DCF mechanisms.

- PCF makes use of an access point that controls medium access and polls the single nodes.
- But ad hoc networks cannot use this function and hence it does not provide QoS rather supports best effort services in IEEE 802.11 WLANs.
- **Refer Fig. 3.6.7.** It shows contention free access using polling mechanisms. Many stations with their NAVs are shown in Fig. 3.6.7.
- The point co-ordinator in the access point splits the access time into super frame periods.
- Super-frame consists of a contention free period and contention period.



(SD15)**Fig. 3.6.7 :Contention free access using polling mechanisms(PCF)**

☞ **Working**

- At time t_0 the contention free period of the super frame should start but as another station is still transmitting the data, the medium is busy.
- Hence the start of the super frame is postponed till t_1.
- The point coordinator waits for PIFS duration and then starts accessing the medium. No other station can start sending earlier as PIFS is smaller than DIFS.
- Now the point coordinator sends data D_1 downstream to the first wireless station. The wireless station can answer after SIFS. After the waiting period of SIFS, the point coordinator again polls the second station by sending D_2.
- This station may answer upstream to the coordinator with U_2. Now the polling continues for third station. But this time the station has nothing to answer and hence the point coordinator will not receive ant packet after SIFS.
- The point coordinator can resume the polling station after the waiting interval of PIFS.
- Finally, the point coordinator issues the end marker (CF_{end}).
- It indicates that the contention period is starting again. Once the contention period is over (after t_3) the next super frame starts, and the above process starts again.
- The contention period can be used for BASIC- DFWMAC or DWFMAC with RTS/CTS.

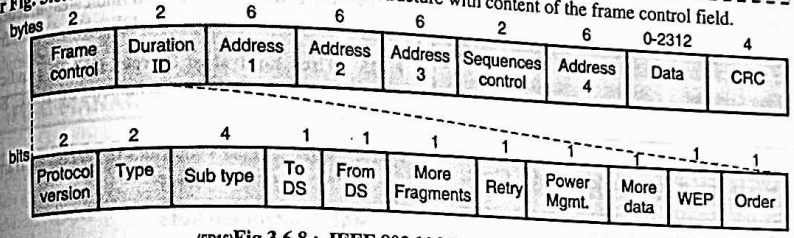
☞ **Disadvantage**

Overhead becomes an issue in case when nodes have nothing to send but access points are polling them permanently.

3.6.4 MAC Frames

Q. Describe MAC frame structure for IEEE 802.11.

Refer Fig. 3.6.8. It shows the basic MAC data frame structure with content of the frame control field.



(SD16)**Fig 3.6.8 : IEEE 802.11 MAC frame structure**

The fields in the data frame are as follows :

1. Frame control	2. Duration/ID	3. Address 1 to 4	4. Sequence control
5. Data	6. Checksum (CRC)	7. Protocol version	8. Type
9. Subtype	10. To DS/from DS	11. More fragments	12. Retry
13. Power management	14. More data	15. Wired equivalent privacy (WEP)	
16. Order			

1. Frame control

- This field carries the instructions on the nature of the packet.
- It distinguishes data from control and management frames. Frame control contains several sub-fields.

2. Duration/ID

- When the value of this field is less than 32,768, the duration of the field indicates the period in which medium is busy.
- It is used for setting the NAV for the virtual reservation mechanism using RTS/CTS and during fragmentation.
- The values above 32768 are reserved for identifiers.

3. Address 1 to 4

- It contains standard IEEE Mac addresses 48 bit each. The meaning of each address is specified by the DS bits in the frame control field.
- MAC frames can be transmitted :
  - between mobile stations
  - between mobile station and access point
  - between access points using DS
- The two bits within Frame Control field **to DS** and **From DS** differentiate these cases and define the four address fields.

Table 3.6.1 : Interpretation of the MAC addresses in an 802.11 MAC frame

Scenario	To DS	from DS	address 1	address 2	address 3	address 4
Ad hoc network	0	0	DA	SA	BSSID	-
Infrastructure network, from AP	0	1	DA	BSSID	SA	-
Infrastructure network, to AP	1	0	BSSID	SA	DA	-
Infrastructure network, within DS	1	1	RA	TA	DA	SA

Refer Table 3.6.1, it shows interpretation of the MAC addresses in an 802.11 MAC frame.

Note
DS : Distribution System,
AP : Access Point,
DA : Destination Address,
SA : Source Address
BSSID : Basic Service Set Identifier,
RA : Receiver Address,
TA : Transmitter Address

- Address 1 identifies the physical receiver. Every station, access point or wireless node filters on address 1.
- Address 2 represents the transmitter of a frame.
- Address 3 and Address 4 are mainly necessary for the logical assignment of frames.

4. **Sequence control :** Sequence number is used to filter duplicate frames.
5. **Data :** The Mac frame may contain arbitrary data max upto 2312 bytes which is transmitted by sender to the receiver transparently.
6. **Checksum (CRC) :** It is 32 bit field and is used to protect the frame.
7. **Protocol version :** It is of 2 bits. It indicates the current protocol version and is fixed to 0 by now.
8. **Type :** It determines the functions of the frame. Each type has several subtypes as well. Types are as defined in Table 3.6.2.

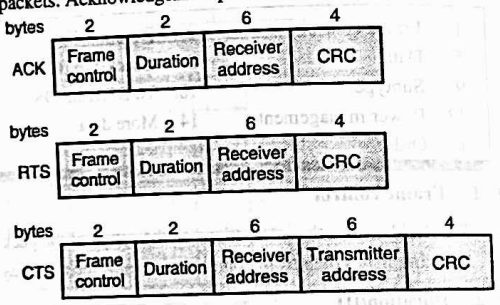
Table 3.6.2 : Types of frame functions and bits allocated

Bits	Type (function of the frame)
00	Management
01	Control
10	Data
11	Reserved

9. **Subtype :** Values 0000 for association request, 1000 for beacon, 1011 for RTS control frame, 1100 is for CTS frame. User data transmits with 0000 subtype.
10. **To DS/From DS :** Used to control meaning of the address field in the MAC frame.
11. **More fragments :** Value 1 represents that there are more data or management fragments of the current MSDU to follow.
12. **Retry :** This field is set to 1 if the frame is the retransmission of previous frame.
13. **Power management :** Value 1 indicates the station goes in power save mode, 0 represents the station remains active.
14. **More data :** This field indicates a receiver that sender has more data to send than the current frame.
15. **Wired Equivalent Privacy (WEP) :** Indicates that the standard security mechanism of IEEE 802.11 is used.
16. **Order :** Value 1 indicates the received frames must be processed in strict order.

MAC Control packets

Fig. 3.6.9 shows three different types of control packets: Acknowledgement packet, RTS, and CTS packet.



(5017)**Fig. 3.6.9 : IEEE 802.11 Special control packets ACK, RTS, CTS**

1. Acknowledgement packet

- The ACK packet is used to acknowledge the correct reception of the data frame.
- The receiver address is directly copied from the address 2 field of the previous frame.
- If there are no fragments to follow, the duration field is set to zero otherwise the duration field is the duration of the previous frame.

2. RTS (Request to Send) packets

- For MACA algorithm RTS/CTS packets are needed.
- These packets are used to reserve the medium to avoid collision.
- Therefore, RTS packet comprises of the receiver address is the address of the intended recipient and the transmitter address.
- The duration field indicates the time to send CTS, data and ACK plus three SIFS.

3. CTS (Clear to Send) packet

- CTS frame copies the transmitter address from the RTS packet into its receiver address field.
- After reading the duration field, it subtracts the time to send the CTS and SIFS and writes the results into its own duration field.

3.7 MAC MANAGEMENT

GQ. Explain synchronization in 802.11 MAC management layer for both infrastructures as well Ad-hoc WLANs.
GQ. Explain power management in IEEE 802.11 infrastructure networks and ad-hoc networks.

MAC management controls all the functions related to system integration. This means the integration of wireless station into BSS, formation of an ESS, synchronization of stations etc.

Following are the function groups

1. Synchronization
2. Power management
3. Roaming
4. Management information base (MIB)

1. Synchronization

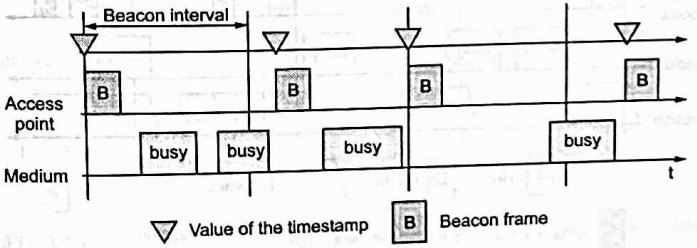
- It includes the functions related to finding of wireless LAN, synchronization of internal clocks, generation of beacon signals etc.
- Each node of an 802.11 network maintains a internal clock. To synchronize the clocks of all nodes, IEEE 802.11 specifies a Timing Synchronization Function (TSF).
- These synchronized clocks are needed for :
  1. Power management
  2. Coordination of the PCF and
  3. Synchronization in FHSS hopping sequence
- Using PCF the local timer of the node can predict the start of a super frame. It means the start of the contention free and the contention period.

Beacon frame

- It contains the time stamp or other management information used for power management and roaming.
- This beacon frame is used within BSS for conveying timing information.
- This time stamp is used by node to adjust its local clock.
- For synchronization, node is not required to hear to every beacon frame, but internal clocks should be adjusted periodically.
- If the medium is busy, the beacon frame is deferred. Therefore, the transmission of the beacon frame is not always periodic.

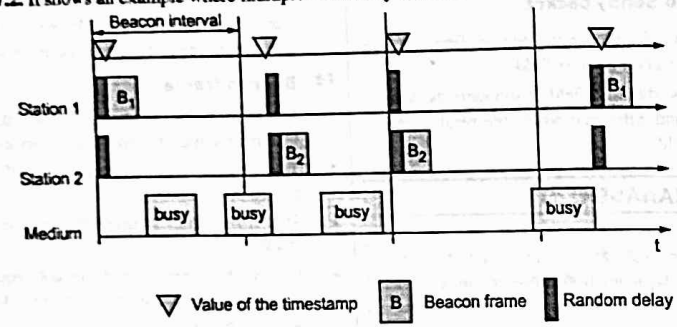
Synchronization process for infrastructure-based networks

- In infrastructure-based networks, an access point controls the synchronization process. It is done by transmitting **beacon frame** periodically.
- Other wireless nodes adjust their local clocks according to beacon time stamp.
- **Refer Fig. 3.7.1.** It shows the beacon transmission in a busy 802.11 infrastructure network.
- AP cannot always assure to send its beacon B signal periodically if the medium is busy.
- However, AP always tries to schedule transmissions according to expected beacon interval. It is known as target beacon transmission time.
- The timestamp of the beacon indicates the actual transmission time and not the scheduled time. Synchronization process for ad hoc networks.
- In this each node maintains its own synchronization timer and starts transmission of a beacon frame after the beacon interval.



(5018)**Fig. 3.7.1 : Beacon transmission in a busy 802.11 infrastructure network**

- **Refer Fig. 3.7.2.** It shows an example where multiple stations try to send their beacon frames.

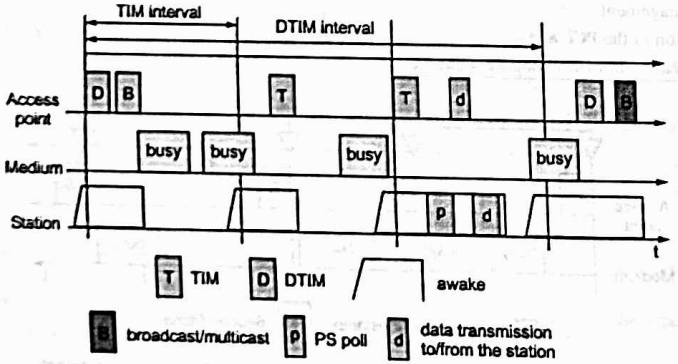


(5019)**Fig. 3.7.2 : Beacon transmission in a busy 802.11 ad-hoc network**

- But the standard backoff algorithm is used so that only one beacon frame is used at a time.
- All the other nodes adjust their internal clocks according to received beacon and suppress their beacons for this cycle. In case of collision, beacon is lost. In this case the beacon interval is shifted slightly.

2. Power management

- In IEEE 802.11 power management, the transceiver is switched off for the duration whenever it is not needed.
- This is simple in case of transmitter as the triggering device it itself whereas it is difficult in case of receivers.
- The receiver can't know in advance when to switch off.
- Switching off the transceiver should be transparent to existing protocols and should be flexible enough to support different applications.
- Longer off periods can save the battery life but on the other hand it reduces the average throughput and vice versa.
- There are two states involved in power saving
  (i) Sleep and Awake (ii) Buffering of data in senders
- If the station is asleep, the sender intending to communicate with the power saving station has to buffer the data.
- The sleeping station has to wake up periodically and needs to stay awake for certain time. During this interval all the senders can announce the destinations of their buffered packets.
- Once the station detects that it is the destination for the buffered packet, it needs to stay awake till transmission takes place. TSF (timing synchronization function) is needed for waking up at the right moment. All the stations need to be awake at the same time.

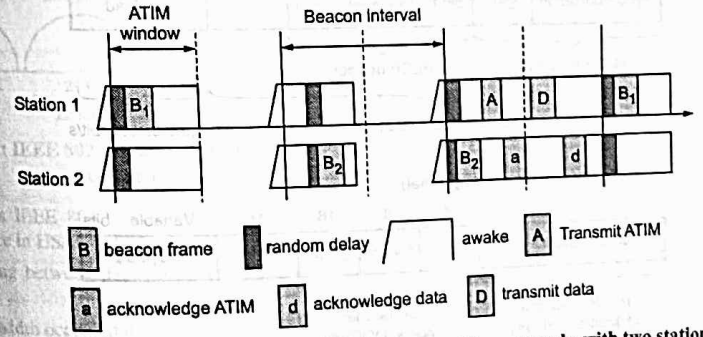


(5020)**Fig. 3.7.3 : Power management in IEEE 802.11 infrastructure networks**

- Power management in infrastructure-based architectures. It is simpler. The AP buffers all the frames intended for the power saving stations.
- Along with beacon frame AP also transmits TIM (time indication map). TIM contains the list of stations for which unicast data frames are buffered in the access point.
- TSF ensures that sleeping stations will wake up periodically and will listen to the beacon frame and TIM.
- For multicast/ broadcast transmission, nodes have to be awake always.
- A frame is also sent from the node to the access point. For this also nodes need to be awake.
- **Refer Fig. 3.7.3.** It shows power management in IEEE 802.11 infrastructure networks.
- **Fig. 3.7.3** shows power management in IEEE 802.11 infrastructure networks. **Fig. 3.7.3** shows power management in IEEE 802.11 infrastructure networks.
- It shows one access point and one station. The state of the medium is also shown in this.
- AP sends the beacon frame at each beacon interval. The beacon interval is same as that of TIM interval.
- The AP also maintains Delivery Traffic Indication Map (DTIM). This is used for sending multicast/ broadcast frames. DTIM is multiple of TIM.
- As shown in the Fig. 3.7.3, all stations are awake to receive the broadcast frame.
- Once the station receives this frame, it again goes into sleeping mode. Once again, all stations wake up before the next TIM transmission.
- If the medium is busy, TIM is delayed. Hence the station stays awake. The AP has nothing to send and therefore station again goes to sleep mode.
- At the next TIM interval, AP indicates that the station is the destination for the buffered frame and hence station answers to this with PS (Power Saving) poll. It then stays awake for reception
- AP then transmits the data for the station. Station acknowledges the receipt and may also send some data. This data is acknowledged by AP. And station goes into sleep mode again.
- Now the AP has large broadcast data to send at the next DTIM interval. This is again delayed as the medium is busy.
- Based on interval thresholds a station may stay awake if the sleeping period is too short. This mechanism clearly shows the trade off between short delays in station access and saving battery power.
- The shorter the TIM interval, shorter is the delay but lower is the power saving effect.

Power management in ad hoc networks

- It is complicated as compared to infrastructure-based networks. In this all the stations have the ability to buffer the data if it wants to communicate with power saving node.
- All stations announce the list of buffered frames during the period when all the stations are awake.
- Destinations are announced using Ad hoc Traffic Indication Map (ATIMs). The announcement interval is known as ATIM window.
- **Refer Fig. 3.7.4.** It shows the power management in IEEE 802.11 ad hoc networks with two stations.
- The beacon interval is determined by the distributed function in which different stations can send the beacon.



(5021)**Fig. 3.7.4 : Power management in IEEE 802.11 ad hoc networks with two stations**

- Due to this all the stations wake up at the same time and they remain awake for ATIM interval.
- If no frame is buffered to them, these stations goes to sleep. This happens in first two steps.
- In the third step, station 1 has data buffered for station 2. It is shown by the ATIM transmitted by ATIM from station1.
- Station 2 acknowledges this ATIM and stays awake for transmission.
- Once the ATIM window is complete, station 1 can transmit and station 2 acknowledges its receipt. In this case stations stay awake for next beacon.

☞ Disadvantages

- More ATIM transmissions results in collision.
- The access delays of large networks are difficult to predict.
- QoS guarantees can't be given under heavy load conditions.

☞ 3. Roaming

- Wireless networks in the building require more than single AP to cover all the rooms. AP has the transmission range of 10-20m. each floor of building also need one AP.
- Moving between the AP is known as roaming.
- The steps of roaming procedure are as follows
- If the current link quality is detected to be poor by station, it starts scanning for another AP.
- It is actually search of another BSS or setting up of new BSS in case of ad hoc networks.
- There are two types of scanning
  - i. **Active scanning :** It involves sending the probe on each channel and waiting for the response
  - ii. **Passive scanning :** it means listening to the medium to find other networks.
- The station selects the best AP and sends the association request to the selected access point.
- This new AP responds with association response. If the response is successful, the station is roamed to new AP else station continues scanning.
- Acceptance od association request by AP indicates new station in its BSS to the Distribution System (DS).
- DS then updates its database of current location of stations. It also informs old AP that the station is no longer exist in its BSS.

⏭ 3.8 802.11B

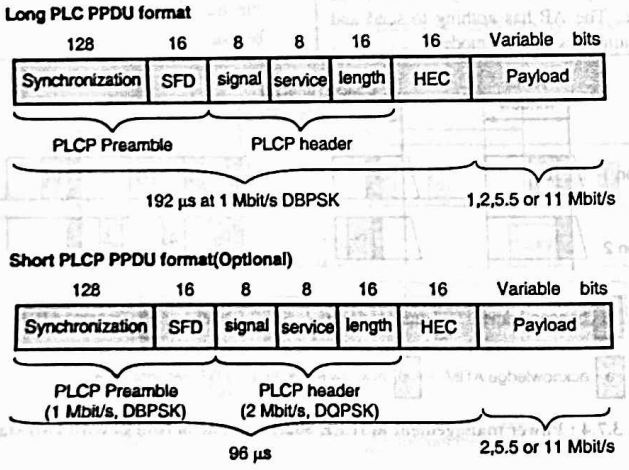
This standard only defines new PHY layer. All the MAC schemes , MAC managements schemes etc. are same as that of IEEE 802.11.

☞ Features

1. Data rate : 11, 5.5, 2 or 1 Mbps
2. Lower data rates use barker codes.
3. Modulation used: DBPSK or DQPSK or CCK

☞ Packet format for IEEE 802.11b

Refer Fig. 3.8.1. It shows the standardized format for 802.11b. in this the mandatory format is known as long PLCP PPDU. It is similar to IEEE 802.11 PHY layer DSSS format.



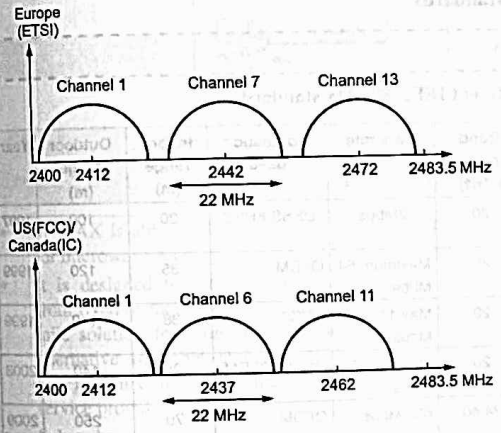
(5D34)**Fig. 3.8.1 : IEEE 802.11b PHY packet formats**

- The only difference in the signal field. In this the rate is encoded in multiples of 100kbps.
- Table 3.8.1 represents the relation between the field value and data rate.

Table 3.8.1 : Field value and data rates

Field value	Data rate
0x0A	1Mbps
0x14	2 Mbps
0x37	5.5 Mbps
0x6E	11 Mbps

- The short PLCP PPDU format differs in many ways.
  1. **Short synchronization field :** contains 56 scrambled zeros.
  2. **SFD :** it contains the mirrored bit pattern 0000010111001111.
- The length of the overhead is only half for the short frames. This is suitable for short but time critical data transmissions.
- Non overlapping channel selection in IEEE 802.11b. Refer Fig. 3.8.2.



(5D35)**Fig. 3.8.2 : IEEE 802.11b non-overlapping channel selection**

- It provides IEEE 802.11b installation with minimum interference in US/Canada and Europe.
- The spacing between the center frequencies: 25 MHz atleast
- The bandwidth occupied by the main lobe: 22 MHz.
- Users can install the overlapping cells for WLANs using the three non overlapping channels to provide seamless coverage.

⏭ 3.9 802.11A

☞ Features

1. Data rate : 54 Mbps
2. Makes use of OFDM
3. Maximum transmit power : 200mW EIRP for lower frequency band (indoor use) 1W EIRP for higher frequency band (for indoor and outdoor use)
4. Number of subcarriers used : 52 (48 data+ 4 pilot)
5. Spacing between the subcarriers: 312.5kHz

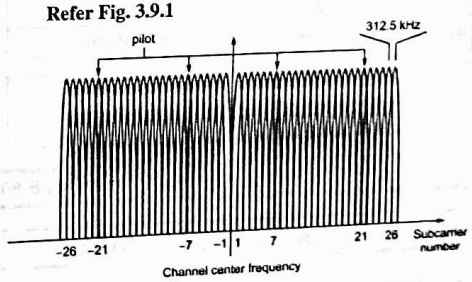
- **Modulation used :** BPSK, QPSK, 16-QAM or 64-QAM
- Different coding schemes are used for different modulation schemes used. Refer Table 3.9.1.

Table 3.9.1 : Rate dependent parameters for IEEE 802.11a

Data rate (Mbit/s)	Modulation	Coding rate	Coded bits per subcarriers	Coded bits per OFDM symbol	Data bits per OFDM symbol
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

☞ OFDM in IEEE 802.11a

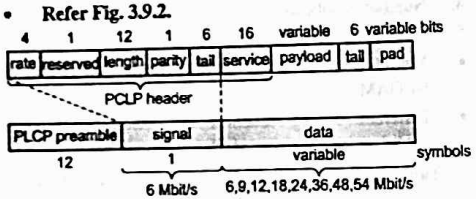
Refer Fig. 3.9.1



(5D22)**Fig 3.9.1 : Usage of OFDM in IEEE 802.11a**

- OFDM is multicarrier modulation scheme. In this symbol rate is reduced by distribution of bits over multiple subcarriers.

- 802.11a use fixed symbol rate of 250000 symbols per second independent of data rate.
- It shows 52 subcarriers are equally spaced around the center frequency (26 on right and 26 on left). The spacing between the subcarriers is 312.5 kHz.
- Subcarriers with numbers -21, -7, 7 and 21 are used as pilot signals.
- IEEE 802.11 a physical layer PDU
- **Refer Fig. 3.9.2.**



(SC23)**Fig. 3.9.2 : IEEE 802.11a physical layer PDU**

1. **PLCP preamble :** it consists of 12 symbols. It is used for frequency acquisition, channel estimation and synchronization. The duration of the preamble is 16µs.
2. **Signal :** it consists of
   - (i) **Rate :** it is 4 bit field. It determines the data rate and modulation of the rest of the packet.
   - (ii) **Length :** it is 12 bit field. It indicates the number of bytes in the payload field.
   - (iii) **Parity :** it is 1 bit field. It shall be even parity for first 16 bits of the signal field.
   - (iv) **Tail :** it is 6 bit field. They are set to zero.
3. **Data :** it is sent with the rate determined in the rate field. It contains following fields.
   - (i) **Service :** it is 16 bits. It is used to synchronize the descrambler of the receiver.
   - (ii) **Payload :** it contains MAC PDU.
   - (iii) **Tail :** it is of 6 bits. They are used to reset the encoder.
   - (iv) **Pad :** it is used to ensure that the number of bits in the PDU maps to an integer number of OFDM symbols.

3.9.1 Comparison of Different IEEE 802.11x Standards

GQ. Compare various IEEE 802.11x standards. (a/b/g/i/n etc.)

Table 3.9.2 : Comparison of different IEEE 802.11x standards

IEEE 802.x standard	Description	Frequency spectrum	Band width (MHz)	Data rate	Modulation used	Indoor range (m)	Outdoor range (m)	Year
IEEE 802.11	Standard for WLAN operation	2.4GHz ISM band	20	2Mbps	DSSS,FHSS	20	100	1997
IEEE802.11a	Standard for WLAN operation	5GHz unlicensed national infrastructure (UNI) band	20	Maximum 54 Mbps	OFDM	35	120	1999
IEEE802.11b	Standard for WLAN operation	2.4GHz ISM band	20	Max 11 Mbps	DSSS	38	140	1999
IEEE802.11g	High rate extension to 802.11	2.4GHz ISM band	20	Maximum 54 Mbps	DSSS, OFDM	38	140	2003
IEEE 802.11 n	Physical/MAC: enhancement to increase throughput	2.4 GHz, 5GHz	24,40	600 Mbps	OFDM	70	250	2009

Syllabus Topic : IEEE 802.16(WiMax) – Mesh Mode

3.10 WMAN / IEEE 802.16 /WIMAX

- Wireless Metropolitan Area Network (MAN) is the name trademarked by the IEEE 802.16 Working Group. It is invented in the year 2001.
- This group focuses on Broadband Wireless Access Standards for its wireless metropolitan area network standard. The standard is popularly known as WiMAX.

- They are developed for providing last mile connectivity for broadband internet access. It is generally focused on home, small business organisations etc. Connectivity.
- It supports multimedia file sharing etc.
- This standard comprises of many IEEE 802.16.x protocols.

Features of IEEE 802.16 WMAN standards

1. Operating frequency : 10 – 66 GHz
2. Bit rate : 32 - 134 Mbps at 28 MHz
3. Modulation used : QPSK, 16 QAM and 64 QAM
4. Bandwidth : maximum 28 MHz

3.10.1 WiMAX

GQ. Explain in detail Wi-Max Technology.

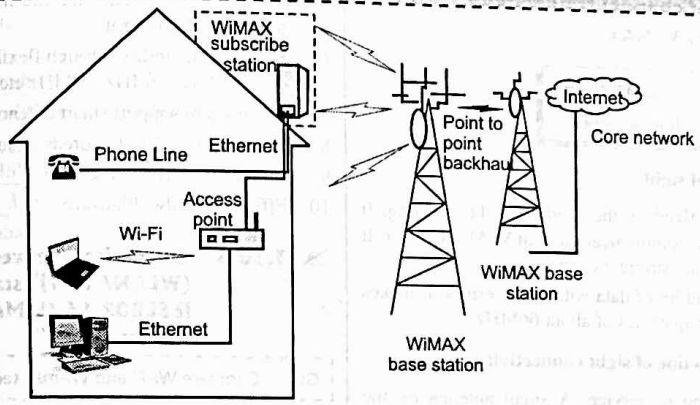


Fig. 3.10.1 : Architecture of WiMAX

- WiMAX is abbreviated for worldwide interoperability for microwave access.
- It is designed to provide broadband Internet access from fixed or mobile devices via antennas. It is the last mile solution for wireless broadband access. It is an alternative to cable and DSL (Digital Subscriber's Line). Hence it is said that WiMAX is IP centric service provided over wide area.
- Subscriber stations communicate with base-stations that are connected to a core network.
- It is a good alternative to fixed line networks. It is simple to build and relatively inexpensive.
- Refer Fig. 3.10.1. It shows general architecture of WiMAX.
- WiMAX supports very high bandwidth solutions where large spectrum deployments (i.e. >10 MHz) are desired. It also reduces the cost as no cables are involved.
- The Architecture of the WiMAX comprises of :
  1. Core network
  2. BS (Base station)
  3. SS (Subscriber station)
  4. TE (Terminal equipment)

1. Core network

It is the standard internet network. It provides the platform for the broadband connectivity.

2. BS (Base station)

- It is the WiMAX cell site. They are the towers with antennas equipped over it. It provides connectivity with the public network. The communication between the subscriber station and the base station is two-way.
- Uplink connection is from SS to BS and downlink connection is from BS to SS.
- A single BS can cover upto 3000 Sq. miles of area.

3. SS (Subscriber station)

- It is the subscriber station equipped with an antenna. This antenna is usually mounted on building.
- It is connected to the base station via microwave links.

4. TE (Terminal equipment)

It can be any device like mobile, laptop etc. It is connected to the subscriber station via access point. The telephone is connected to the subscriber station via Ethernet.

Two types of channel connectivity supported by WiMAX

1. LOS (line of sight)
2. NLOS (non line of sight)

1. LOS (line of sight)

- An antenna is fixed on the rooftop of the building. It has line of sight communication with WiMAX tower. It is more stable and stronger connection.
- It is able to send lot of data with fewer errors. It makes use of higher frequencies of about 66MHz.

2. NLOS (Non line of sight connectivity)

It is Wi-Fi kind of service. A small antenna on the computer connects to the tower. It uses lower frequency range of about 2 to 11GHz.

Features of WiMAX

1. It uses wireless link with microwaves or millimetre waves.
2. Uses licensed spectrums.
3. Simple stationary antennas tower mounted antennas
4. It is connection oriented wide area service.
5. Supports high bandwidth and hundreds of users per channel.
6. Range : 30 miles
7. It is capable of providing broadband access to remote places.
8. Makes use of point to multipoint architecture.
9. Provides broadband and quality of service guarantee data transmissions

3.10.2 IEEE 802.16a Standard

- Few advancements in the physical layer of IEEE 802.16 are to done and IEEE802.16a is standardised. This is done to meet growing BWA (broadband wireless access) demand.
- It is developed to give access of high-speed internet access to home or business organizations.
- It provides good performance in robustness and supports good quality of service.
- It supports NLOS communications.

IEEE 802.16 features/Specifications

1. Operating spectrum : 2 - 11 GHz
2. Connectivity : NLOS (Non line of sight)
3. TDD and FDD duplexing support
4. 256 point FFT OFDM used
5. Ensures a robust RF link and maximizes the data rate for each subscriber unit.
6. Supports flexibility through flexible Channel sizes (e.g. 3.5MHz, 5MHz, 10MHz etc.)
7. Designed to support smart antenna systems
8. Scalable from 1 to hundreds of subscribers
9. Connection-oriented service
10. Efficient bandwidth usage

3.10.3 Comparison between IEEE802.11 (WLAN/ Wi-Fi) standard and IEEE802.16 (WMAN/ WiMAX) standard

GQ. Compare Wi-Fi and Wi-max technology.

Table 3.10.1 : Comparison between IEEE802.11 and IEEE 802.16 standard

Sr. No.	Parameter	IEEE802.11	IEEE802.16
1.	Technology	WLAN	WiMAX
2.	Operating spectrum	2.4 GHz / 5.2GHz	2 - 11GHz / 11-60GHz
3.	Bandwidth	11 - 54Mbps	Upto 70Mbps
4.	Range (LOS)	100m	30 - 50 km
5.	Range (NLOS)	30m	2 - 5 km
6.	Mobility	Portable	Fixed
7.	Data rate	Upto 54Mbps	Upto 150Mbps
8.	Application	Indoor	Outdoor
9.	Protocols supported	802.11a/b/g/n/ac/ad etc.	802.16a/d/e/m etc.
10.	Modulation	OFDM,DSSS	QPSK

3.10.4 Comparison between WPAN, WMAN and WLAN standards

Table 3.10.2 : Comparison between WPAN, WLAN and WMAN standards

Sr. No.	Parameter	WPAN	WLAN	WMAN/ WiMAX
1.	IEEE standard	IEEE802.15	IEEE802.11	IEEE802.16
2.	Standards	Bluetooth	Wi-Fi	Wimax
3.	Operating frequency spectrum	2.4 - 2.483 GHz	2.4 GHz / 5.2GHz	2 - 11GHz/ 11 - 60GHz
4.	Mobility	Portable	Portable	Fixed
5.	Data rate	1 - 4Mbps	Upto 54Mbps	Upto 150Mbps
6.	Modulation	FHSS	OFDM,DSSS	QPSK
7.	Range	1 - 3 m	112 m	Variable
8.	Application	Cable replacements for peripherals	Mobile extension of wired networks	Fixed wireless between homes and businesses and the Internet

Syllabus Topic : IEEE 802.16 (WiMax) – Physical and MAC layer

3.11 PHY AND MAC LAYER IN WIMAX

3.11.1 Physical layer in WiMAX

- The 802.16 PHY supports TDD and full and half duplex FDD operations. Adaptive modulation and coding (AMC) is supported.
- Hybrid automatic repeat request (HARQ) and fast channel feedback (CQICH) schemes are used to enhance coverage and capacity of WiMAX in mobile applications.
- Since the PHY layer design for 2-11 GHz range is complex, burst by burst adaptability for modulation and coding schemes is used.
- There are three different air interfaces used in the range of 2-11 GHz. They are as follows.
- Wireless MAN — SCa uses single carrier modulation.
- Wireless MAN — OFDM uses a 256-carrier OFDM. This air interface provides multiple access to different stations through time-division-multiple access.
- Wireless MAN — OFDM uses a 2048-carrier OFDM scheme. The interface provides multiple access by assigning a subset of the carriers to an individual receiver.
- In the downlink with mobile WiMAX, QPSK, 16-QAM and 64QAM are supported however 64 QAM is optional in uplink.
- Coding schemes supported are convolutional codes and turbo codes Adaptability of data rate is achieved with the help of combinations of various modulation and coding schemes
- The base station (BS) scheduler determines the appropriate data rate for each burst allocation based on the buffer size, channel propagation conditions at the receiver, etc. A channel quality indicator (CQI) channel is used to provide channel state information from the user terminals to the BS scheduler.
- WiMAX supports fully asynchronous operation.

3.11.2 WiMAX-Medium Access Control (MAC) layer

- The MAC layer of WiMAX is designed to support distributed stations with high data rates.
- The 802.16 MAC is a scheduling MAC where the subscriber only has to compete once (for initial entry into the network). After that it is allocated a time slot by the base station.
- The time slot can enlarge and constrict, but it remains assigned to the subscriber
- This scheduling algorithm is stable under overload and oversubscription.
- It is also more bandwidth efficient. The scheduling algorithm allows the base station to control QoS by balancing the assignment among the needs of subscribers.
- MAC layer supports TDD and FDD type of duplexing.
- IEEE 802.16 MAC is connection oriented. It performs link adaptations and ARQ functions to maintain target bit error rate thereby maximizing the data throughput. It supports IPv4, IPv6, Ethernet, and ATM.

Self Learning Topics : WLL(Wireless Local Loop)

3.12 FIXED WIRELESS COMMUNICATION : WLL - WIRELESS LOCAL LOOP

- **Loop :** It is defined as the circuit connecting a subscriber's station that is telephone set with the line terminating equipment in central office. Central office is a switch in the telephone network.