CHAPTER 4

Unit IV

Wireless Local Area Networks

Syllabus

4.1 Wireless Local Area Networks : Introduction, Infrastructure and ad-hoc network

4.2 IEEE 802.11:System architecture, Protocol architecture, Physical layer, Medium access control layer, MAC management, 802.11a, 802.11b

4.3 Wi-Fi security : WEP, WPA, Wireless LAN Threats, Securing Wireless Networks

4.4 HIPERLAN 1 and HIPERLAN 2

4.5 Bluetooth : Introduction, User Scenario, Architecture, protocol stack

Introduction

This chapter introduces another class of wireless network technologies called Wireless Local Area Networks (WLANs). In contrast to the technologies described in the previous chapters such as GSM, GPRS, UMTS etc. WLANs are typically restricted in their diameter to buildings, a campus or a single room and are operated by individuals and not by large scale network providers. The main goal of WLAN is to replace office cabling, to enable tetherless access to the Internet and to allow ad hoc communication. The chapter discusses various WLAN technologies such as IEEE 802.11, HIPERLAN/1 and HIPERLAN/2. For each WLAN system, the details of architecture, the physical layer and MAC layer have been discussed.

Remainder of the chapter focuses on Bluetooth technology and comparison of all of the above mentioned WLAN technologies.

4.1 Wireless Local Area Networks

4.1.1 Introduction

- A wireless LAN (or WLAN, for wireless local area network) is one in which a mobile user can connect to a local area network (LAN) through a wireless (radio) connection.
- The IEEE 802.11, group of standards specify the technologies for wireless LANs.
- Home users can create a wireless network out of an existing wired network and wirelessly extend the reach of the Internet throughout the home on multiple computers.
- By using wireless LAN, it is now not required that every workstation and conference room be wired up to hubs and switches with cables.

Advantages of Wireless LAN

1. **Flexibility :** Within radio coverage, a user can easily communicate without any restriction.
2. **Simplified planning :** Wireless ad-hoc networks do not require any planning for configuring a network.
3. **(Almost) no wiring difficulties :** Because no wiring is required, it can be easily installed where wiring is difficult (e.g. historic buildings, firewalls).
4. **Robust :** Wireless LAN is more robust against disasters like, e.g., earthquakes, fire, or users pulling a plug.
5. **Cost effective :** Once a wireless network is installed, adding new additional user will not increase further cost.

Disadvantages of wireless LAN

1. **Lower bandwidth and transmission quality :** Wireless LAN offers **very low bandwidth** (1-10 Mbit/s) compared to wired networks due to shared medium. Also it has high error rates due to interference. Hence it offers **low QoS** as compared to wired network.
2. **Many proprietary solutions** exist, due to slow standardization procedure.
3. **Local regulatory restrictions :** Several countries impose different spectral restrictions. Due to this it is difficult to establish global WLAN solutions.
4. **Lower safety and security :** Security concerns are high in wireless networks. The open radio interface makes eavesdropping much easier in WLANs than wired network.

4.1.2 Types of WLAN

Based on the network configuration, wireless LANs can be classified into two categories.

1. Infrastructure based wireless networks
2. Ad hoc wireless networks

1. Infrastructure based wireless network

- An important element of this type of network is Access point (AP).
- AP provides an interface between the wireless terminals and wired network infrastructure.
- Here wireless nodes communicate with each other via an access point.
- All the network control procedures like medium access control, synchronization, power management has been done by the AP.
- Fig. 4.1.1 shows three access points with three wireless networks and a wired network.
- The design of infrastructure based wireless network is very simpler than ad-hoc networks. Since AP performs most of the transmission control procedures, the complexity of individual node is less.
- Infrastructure based wireless network is less flexible. For example, in the case of disaster they cannot be used when no infrastructure is left.
- For Example, Cellular phone network.

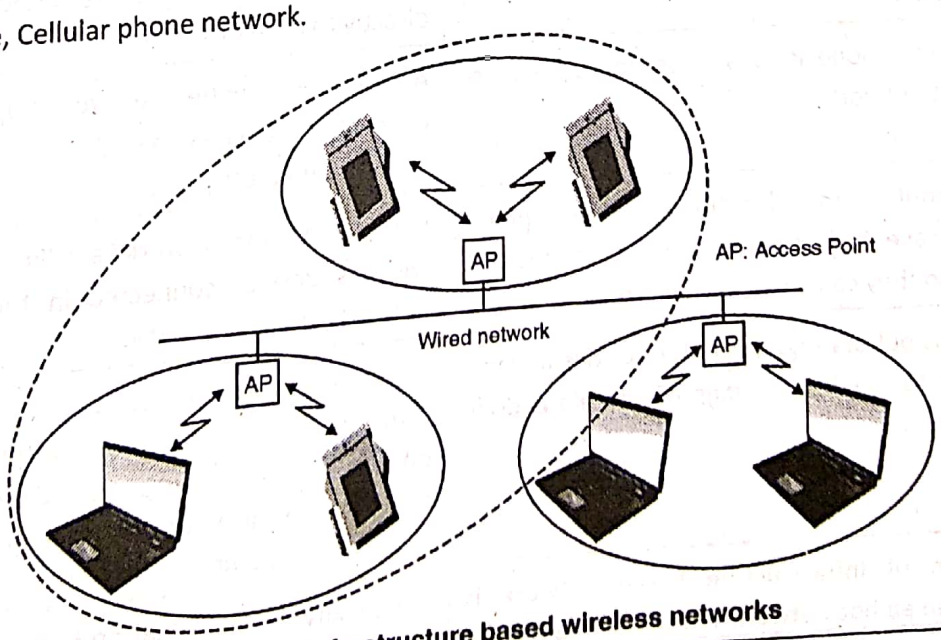


Fig. 4.1.1 : Infrastructure based wireless networks

2. Ad-hoc wireless networks

- Ad hoc wireless networks do not have any wired infrastructure.
- All nodes can communicate directly without need of access point.
- The complexity of nodes in an ad-hoc network is higher because all network functionalities like medium access mechanisms, which hidden and exposed terminal problems have to be implemented within the node itself.
- Fig. 4.1.2 shows two ad-hoc networks with three nodes each.

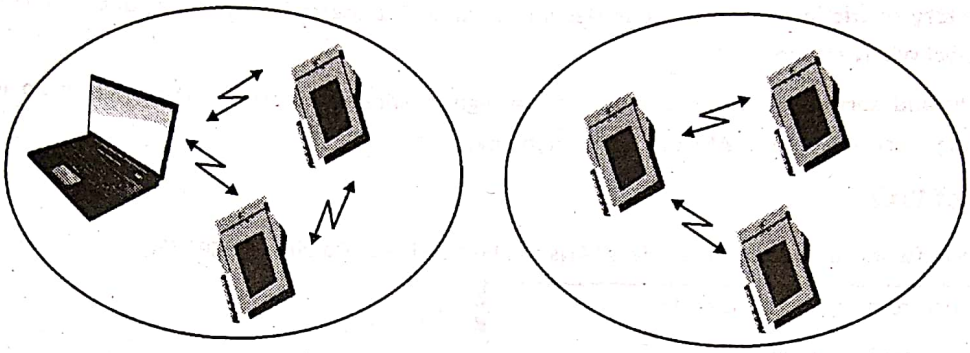


Fig. 4.1.2 : Ad-hoc wireless networks

- In ad hoc networks, nodes can only communicate when they are within each other's radio range or if other nodes can forward the message.
- It offers higher flexibility as these networks can be installed instantly without need of any infrastructure.

4.1.3 Difference between Ad-hoc Network and Infrastructure based Wireless Networks

MU – Dec. 15

Q. Explain Difference between Ad-hoc Network and Infrastructure based Wireless Networks. **(Dec. 15, 5 Marks)**

Sr. No.	Infrastructure based Network	Ad-hoc networks
1.	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.	Infrastructure mode is ideal if setting up a more permanent network.	Ad-hoc mode can be easier to set up if you just want to connect few devices to each other without requiring a centralized access point.
3.	Wireless routers that function as access points generally have higher-power wireless radios and antennas so they can cover a wider area.	Range of Ad-hoc networks are limited by the power of wireless devices connected in the network. Ad-hoc networks don't scale well.
4.	If a device is out of range of another device it wants to connect to, then forwarding of packets is done via access point.	If a device is out of range of another device it wants to connect to, it will pass the data through other devices on the way. Passing the data through several computers is just slower than passing it through a single access point.
5.	The design of infrastructure based network is simpler than ad hoc networks, since an access point	Complexity of individual node in ad hoc networks is higher because all network functionality such as

Sr. No.	Infrastructure based Network	Ad-hoc networks
	performs most of the transmission control procedures, thus reducing the complexity of individual node.	medium access mechanism, power management, synchronization etc. have to be implemented within the node itself.
6.	Infrastructure based wireless network is less flexible. For example, in case of disaster, they cannot be used when no infrastructure is left.	It offers higher flexibility as these networks can be installed instantly without need of any infrastructure.
7.	Requires more planning and takes time to set up.	No planning is needed and Easy to set up.
8.	Architecture of Infrastructure based network is shown in Fig. 4.1.1.	Architecture of ad- hoc network is shown in Fig. 4.1.2.

4.2 IEEE 802.11

- **IEEE 802.11** is a set of standards for implementing wireless local area network (WLAN) in 2.4, 3.6 and 5 GHz frequency bands.
- They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802).
- IEEE 802.11 introduced various versions of 802.11 - 802.11a, 802.11b, 802.11g, etc.
- To maintain interoperability, this standard uses the same interface as the others to higher layers, but specifies the **physical layer** and **medium access layer** adapted to the special requirement of wireless LANs.

4.2.1 IEEE 802.11 System Architecture

IEEE 802.11 LANs can be configured as infrastructure based network or as ad hoc networks.

1. Architecture of Infrastructure based network

Fig. 4.2.1 shows the architecture of IEEE 802.11 infrastructure based network.

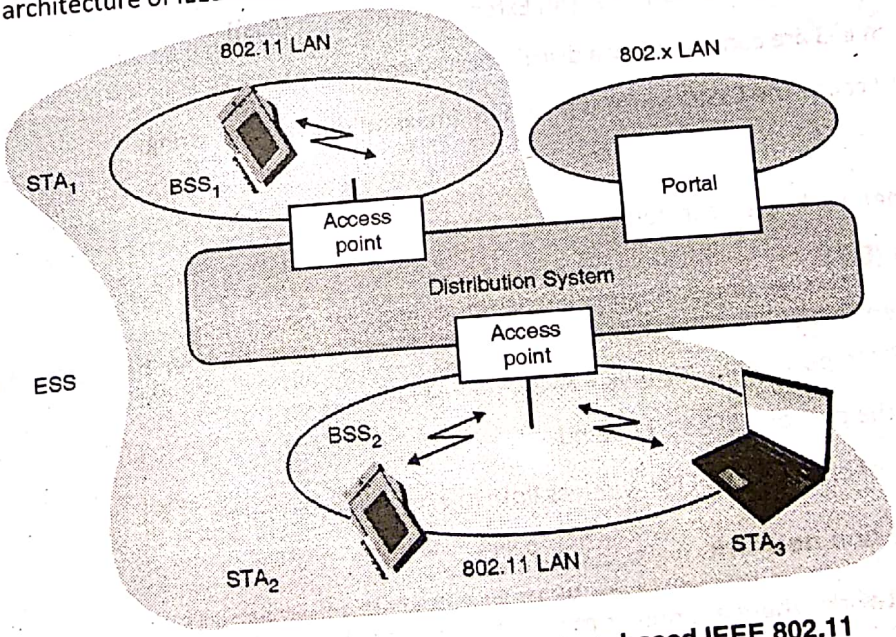


Fig. 4.2.1 : Architecture of an infrastructure based IEEE 802.11

Basic Service Set (BSS)

- The basic building block of IEEE 802.11 architecture is the Basic Service Set (BSS).
- The stations and access point which are within the same radio coverage form a Basic Service Set (BSS).
- All stations within a BSS communicate with the same access point and compete for shared medium.
- Access point can be connected to other access points via distribution system.

Station (STA)

- The station is a wireless node and it is connected to an access point.
- All stations are equipped with wireless network interface cards (WNICs) and contain the functionalities of the 802.11 protocol.
- Wireless station can be mobile devices such as laptops, personal digital assistants, IP phones and other smart phones, or fixed devices such as desktops and workstations that are equipped with a wireless network interface.

Access Point (AP)

- Access points (APs) are base stations for the wireless network.
- Two terminals in the same BSS communicate via AP.
- AP's functions are :
  1. Supports roaming (i.e. changing access points)
  2. Provides synchronization within a BSS
  3. Supports power management
  4. Can control medium access to support time bounded services

Extended Service Set (ESS)

- A set of connected BSSs together form ESS (An Extended Service Set (ESS))
- Access points in an ESS are connected by a distribution system.
- Each ESS has an ID called the ESSID which is a 32-byte (maximum) character string.

Portal

It acts as an internet working unit to connect other LANs.

Distribution System (DS)

- A distribution system works as a backbone network and handles data transfer between different AP's. It connects several BSS's via AP's to portal thus forming a single network.
- The DS is not really the part of IEEE802.11 standard.
- The DS could consist of bridged IEEE LAN wireless links or any other network.

2. Architecture of ad hoc network

In ad-hoc wireless networks, there are one or more independent BSSs (IBSS) as shown in Fig. 4.2.2.

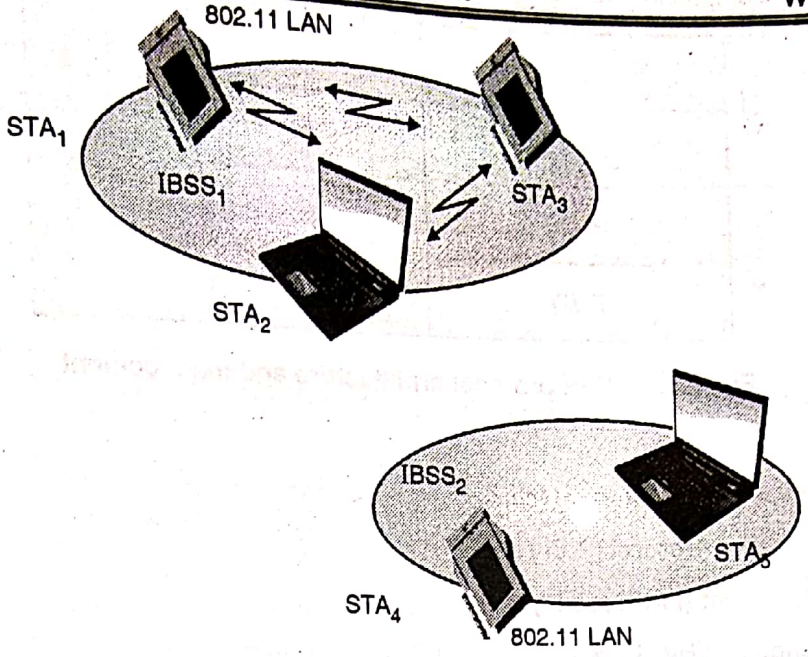


Fig. 4.2.2 : Architecture of IEEE 802.11 ad-hoc wireless LAN

IBSS comprises a group of stations using the same radio frequency. For example, as shown in Fig. 4.2.2 STA_1, STA_2, and STA_3 are in $IBSS_1$, where as STA_4 and STA_5 in $IBSS_2$. This mean, STA_2 can communicate directly with STA_3 but not with STA_4.

4.2.2 IEEE 802.11 Protocol Architecture

MU – May 13

Q. Explain protocol architecture of 802.11. (May 13, 10 Marks)

- As shown in Fig. 4.2.3 an 802.11 wireless LAN connected to a switched IEEE 802.3 Ethernet via a bridge (Access point).
- 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.**

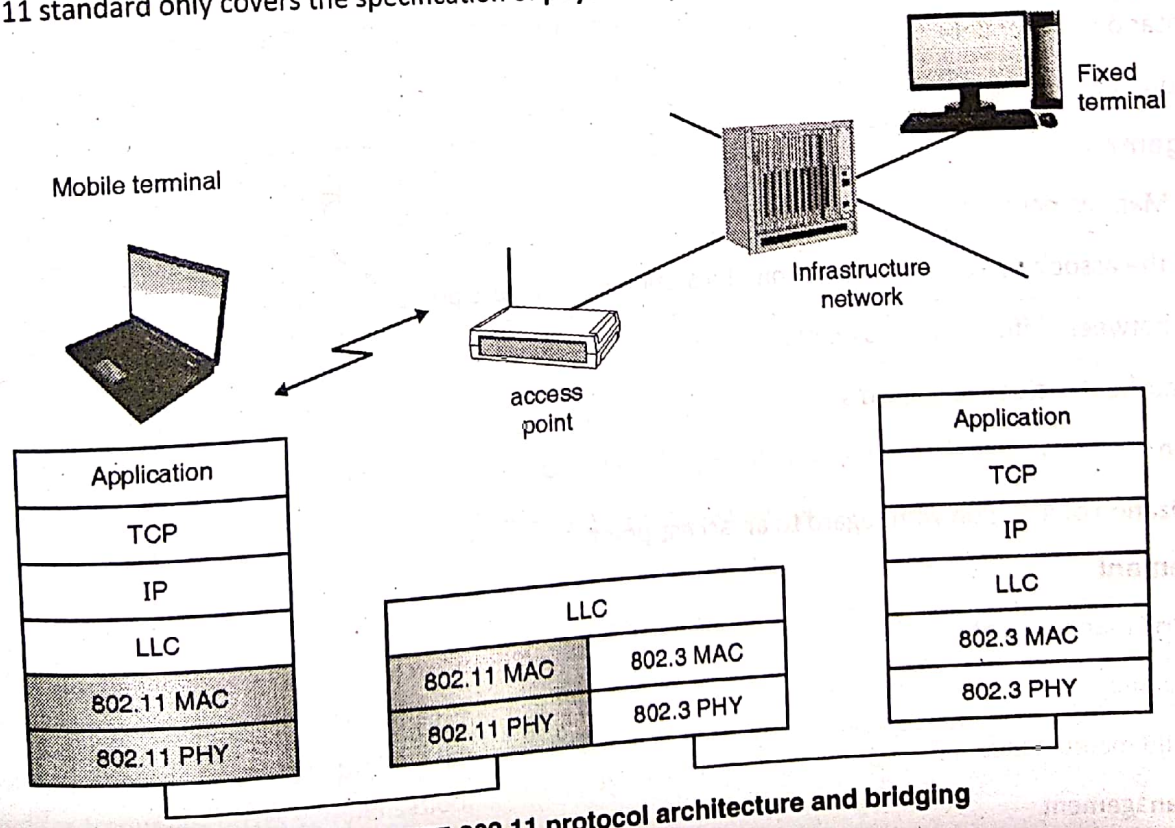


Fig. 4.2.3 : IEEE 802.11 protocol architecture and bridging

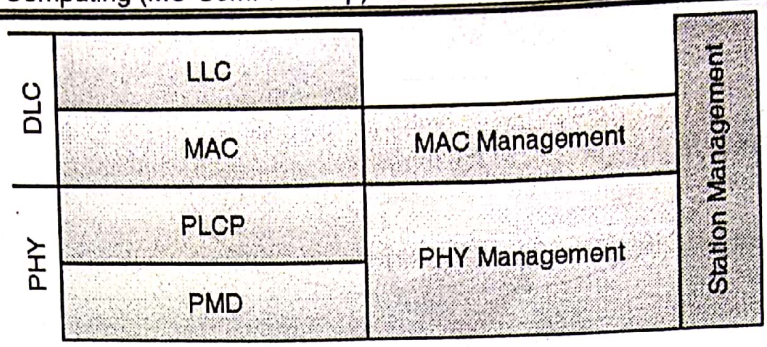


Fig. 4.2.4 : IEEE protocol architecture and management

Physical Layer

- The Physical layer (**PHY**) is subdivided into 2 parts :
  - Physical layer convergence protocol (PLCP) and
  - Physical medium dependent (PMD) sub layer.
- Protocol architecture is shown in Fig. 4.2.4 :
  - The **PLCP** sub layer provides
    - (a) A carrier sense signal, called clear channel assessment (CCA)
    - (b) A common PHY service access point (SAP)
  - The **PMD** sub layer handles
    - (a) Modulation
    - (b) Encoding/decoding of signals

MAC layer

The basic tasks of **MAC** layer :

(a) Medium access

(b) Fragmentation of user data

(c) Encryption of user data

MAC management

Tasks of MAC Management :

(a) Supports the association and re-association of a station to an access point

(b) Roaming between different access points

(c) Controls authentication mechanisms

(d) Encryption

(e) Synchronization of a station with regard to an access point

PHY management

Tasks of PHY management :

(a) Channel tuning

(b) Physical MIB maintenance

(c) Station management

4.2.3 IEEE 802.11 Physical Layer

In basic IEEE802.11 version three different physical layers have been standardized.

(a) DSSS Physical layer (DSSS-PHY)
(b) FHSS Physical layer (FHSS – PHY)
(c) Infra red Physical Layer

4.2.3(a) Direct Sequence Spread Spectrum Physical Layer (DSSS-PHY)

MU – Dec. 14

Q. Discuss the PHY frame format of an IEEE 802.11 using the spread spectrum technique, which separates by code. **(Dec. 14, 10 Marks)**

- This type of physical layer uses radio wave for transmission.
- As the name suggests, it uses direct sequence spread spectrum technique.
- IEEE 802.11 DSSS spreads the signal by using 11 bit barker code (+ 1, – 1, + 1, + 1, – 1, + 1, + 1, + 1, – 1, – 1, – 1).
- It also uses **2.4 GHz** ISM band (same as FHSS) and offers both 1 Mbit/s and 2 Mbit/s data rate.
- It uses Differential Binary Phase Shift Keying (DBPSK) for 1 Mbit/s transmission and Differential Quadrature Phase Shift Keying (DQPSK) for 2 Mbit/s.
- Maximum transmit power is 1W (in the US), 100mW EIRP in the Europe and 10mW/MHz in Japan.
- The symbol rate is 1 MHz and chipping rate is 11 MHz.
- Implementation is difficult.
- Provides a better coverage and a more stable signal (less interference and less multipath propagation).

Frame structure of DS-SS physical layer

- General packet sent over the channel consists of three parts : The PLCP preamble, The PLCP header and the Payload shown in Fig. 4.2.5.

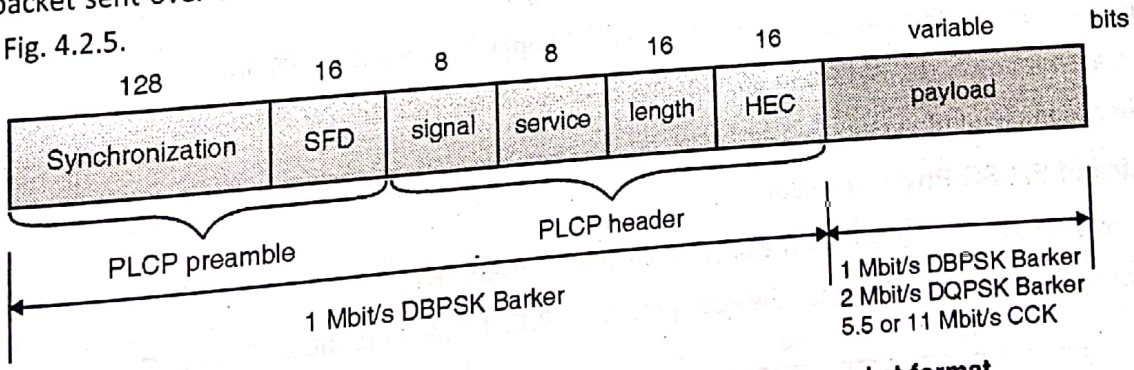


Fig. 4.2.5 : IEEE 802.11 DS-SS PLCP Physical layer packet format

- The DS-SS Physical layer PLCP packet format of IEEE 802.11 is shown in Fig. 4.2.5.
- The PLCP part is always transmitted at the rate of 1 Mbit/s.
- Payload can be transmitted at either 1 or 2 Mbit/s depending upon the modulation technique used.

The fields of a frame have the following functions.

- **Synchronization :** It is a 128 bit field (alternating 0 and 1) used for synchronization, gain setting, energy detection, and for frequency offset compensation.

- **Start frame delimiter (SDF) :** This field indicates the starting of a frame and consist the pattern 1111001110100000.
- **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.
- **Service :** This field is reserved for future use.
- **Length :** This 16 bit field is used to indicate the length of a payload in microseconds.
- **Header Error Check (HEC) :** HEC is used to protect PLCP header.

- The PLCP part of the packet is followed by the payload carrying MAC packet data unit (MPDU) of the length between 1 to 2048 octets.
- Instead of 11–bit Barker code applied with DBPSK or DQPSK modulation, the Complementary Code Keying (CCK) can be used to achieve higher data rates of 5.5 or 11 Mbit/s.
- The DS-SS version of the physical layer ensures high data rate and high range, but is costlier than FH-SS technique due to the high cost of DS-RF components. More over DS-RF components also use more power.

4.2.3(b) Frequency Hopping Spread Spectrum Physical Layer (FHSS – PHY)

- This type of physical layer uses radio wave for transmission.
- As the name suggests, it uses frequency hopping spread spectrum.
- Compared to DS-SS physical layer, FH-SS physical layer provides high distortion immunity, high system capacity, low power use and uses low cost RF components.
- It also uses the **2.4 GHz** ISM band.
- Provides bandwidth of **1MHz**.
- It uses Gaussian Frequency Shift Keying (GFSK) for modulation.
- 2-level GFSK is used for 1 Mbit/s (1 bit is mapped on one frequency). 4-level GFSK is used for 2 Mbit/s (2 bits are mapped on one frequency).
- Operation at 1 Mbit/s is mandatory while at 2 Mbit/s is optional.
- 79 Hopping channels for North America and Europe and 23 hopping channels for Japan.
- Maximum transmit power is 1 W/MHz in US, 100 mW EIRP in Europe and 10mW/MHz in Japan.
- FHSS is easier to implement.

Frame structure of FH-SS Physical layer

- Fig. 4.2.6 shows the frame structure of the physical layer with FH-SS PHY.
- The frame consists of three basic parts : the PLCP preamble, PLCP header and the payload part.

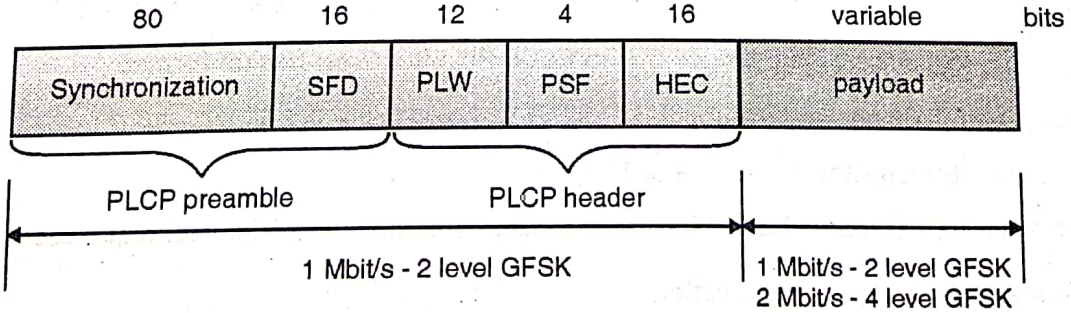


Fig. 4.2.6 : IEEE 802.11 FH-SS PLCP Physical layer packet format

The fields of a frame are as follows :

1. **Synchronization :** This pattern is used for the synchronization of the receivers and signal detection by the CCA (Clear Channel assessment). It is 80 bit field which is a 010101010.... 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 length of a packet could be up to 4k bytes.
4. **PLCP signaling field (PSF) :** 4 bit PSF field 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.

4.2.3(c) Infra Red Physical Layer

- The physical layer uses ***infra red*** for transmission.
- Digital signals are sent using infra red rays of the wave length 850-950nm range and Pulse Position Modulation (PPM).
- Two data rates, 1 and 2 Mbit/s have been standardized.
  - For 1 Mbit/s data rate, transmitted bits are grouped in 4-bit blocks and 16-PPM is applied.
  - For 2 Mbit/s, the data stream is divided into 2-bit blocks and 4-PPM is applied.

Frame structure of Infra red physical layer

The PLCP packet format of Infra red physical layer has been shown in Fig. 4.2.7.

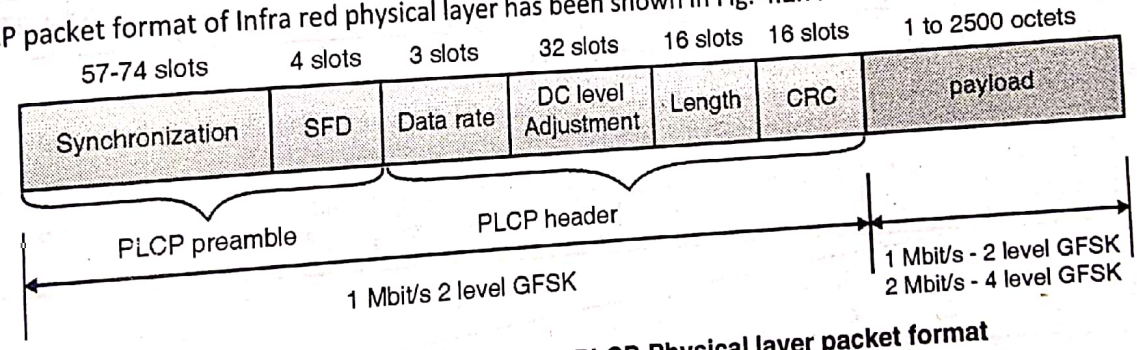


Fig. 4.2.7 : IEEE 802.11 Infrared PLCP Physical layer packet format

- Here the field **DC level adjustment** contains pattern which enables the receiving station to set the DC level of the signal.
- The IR interface is the cheapest of all 802.11 physical interfaces.
- It does not need any frequency regulations.
- It is resistant to eavesdropping. But it has lower coverage.
- As Infra red light interferes with other resources like sunlight or heat sources etc. such networks can only be used within buildings, e.g. classrooms, meeting hall, conference hall etc.
- Frequency reuse is very simple. The same frequency can be used in different classrooms.

MU – Dec. 16

4.2.4 IEEE 802.11 MAC Sublayer

Q. Explain in Detail IEEE 802.11 MAC sublayer. **(Dec. 16, 10 Marks)**

The MAC layer responsibilities are divided between MAC sub layer and MAC layer management sub layer.

- Responsibilities of MAC sub layer :
  - To handle access mechanism
  - Define addressing and frame format
- Responsibilities of MAC layer management sub layer :
  - Roaming in the DSS
  - Power management
  - Authentication
  - Security

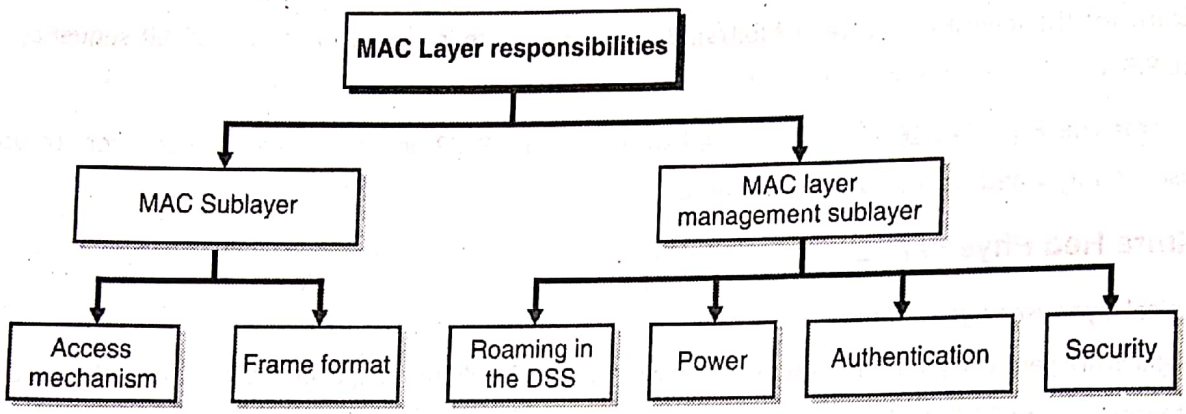


Fig. 4.2.8 : IEEE 802.11 MAC Layer Responsibilities

4.2.4(a) MAC Frame Format

MU – May 14

Q. Explain IEEE 802.11 MAC frame format in detail. **(May 14, 10 Marks)**

Fig. 4.2.9 shows the general MAC frame format of IEEE 802.11.

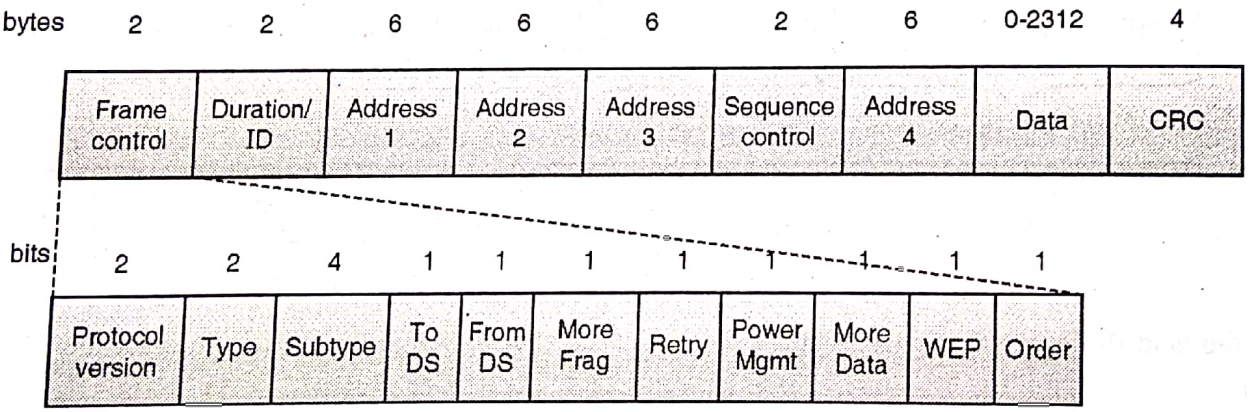


Fig. 4.2.9 : IEEE 802.11 MAC frame format

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. **Protocol version :** Shows the current protocol version and is fixed by 0.
3. **Type :** Determines the functions of a frame: management (00), control (01) and data (10). The value 11 is reserved.
4. **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.
5. **To DS/From DS :** Used to control meaning of the address field in the MAC frame.

6. **More fragments :** Value 1 represents that there are more data or management fragments of the current MSDU to follow.
7. **Retry :** This field is set to 1 if the frame is the retransmission of previous frame.
8. **Power management :** Value 1 indicates the station goes in power save mode, 0 represents the station remains active.
9. **More data :** This field indicates a receiver that sender has more data to send than the current frame.
10. **Wired Equivalent Privacy (WEP) :** Indicates that the standard security mechanism of IEEE 802.11 is used.
11. **Order :** Value 1 indicates the received frames must be processed in strict order.
12. **Duration/ID :** This field is used to define the period of time in which the medium is occupied. This field is used to set NAV in RTS/CTS mechanism.
13. **Address 1 to 4 :** Four address fields (48 bits each) are used to identify the source, destination and access point to which they are connected.
14. **Sequence control :** Used for fragmentation numbering to control sequence numbering.
15. **Checksum :** Used to protect frame.

- 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.

(i) **Address 1** identifies the physical receiver. Every station, access point or wireless node filters on address 1.

(ii) **Address 2** represents the transmitter of a frame.

(iii) **Address 3** and **Address 4** are mainly necessary for the logical assignment of frames.

Table 4.2.1: MAC addresses in IEEE 802.11

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

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

MAC Control packets

Fig. 4.2.10 shows three different types of control packets : Acknowledgement packet, RTS, and CTS packet.

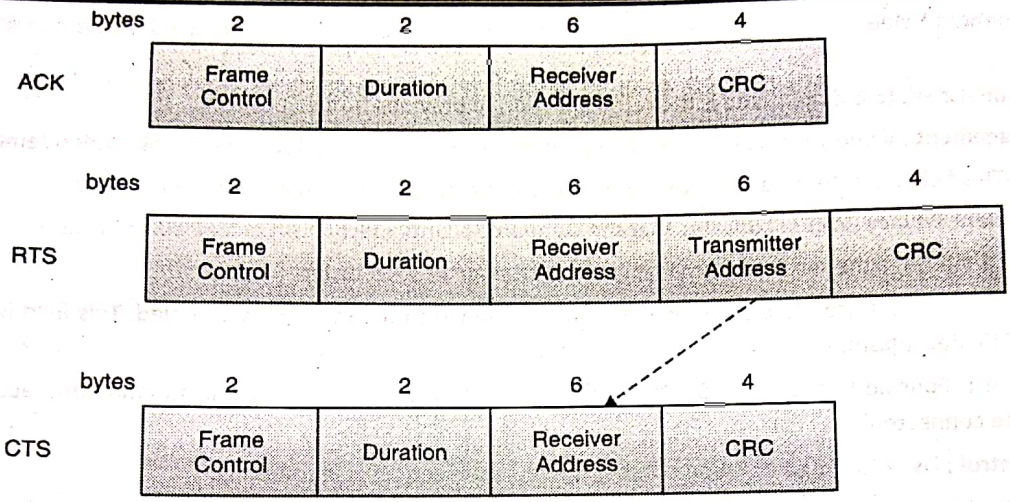


Fig. 4.2.10 : IEEE 802.11 special control packets ACK, RTS and CTS

- RTS packet contains the receiver address of the intended recipient and the transmitter address of the station transmitting the RTS.
- The duration specifies the time required to send CTS, data and its ACK plus three SIFS.
- The immediately following CTS frame copies the transmitter address from the RTS packet in to the receiver address field.

4.2.4(b) Access Mechanisms in IEEE 802.11

IEEE 802.11 offers two types of MAC services,

1. **DCF (Distributed Coordination Function) :** DCF offers only asynchronous data service and it includes two mechanisms.
   - **Contention** mechanism supported by CSMA/CA protocol.
   - **Contention free** mechanism by using RTS/CTS.

   It is mandatory service.
2. **PCF (Point Coordination Function) :** PCF offers asynchronous data service as well as time bounded service. It includes :
   - **Contention free** polling method. It is an optional service.
   - Ad hoc networks can offer only **asynchronous data services** (can only use DCF).
   - Infrastructure based networks can offer both **asynchronous (DCF)** as well as **time bounded services (PCF).**
   - The MAC mechanisms collectively are also called Distributed Foundation Wireless Medium Access Control **(DFWMAC).**

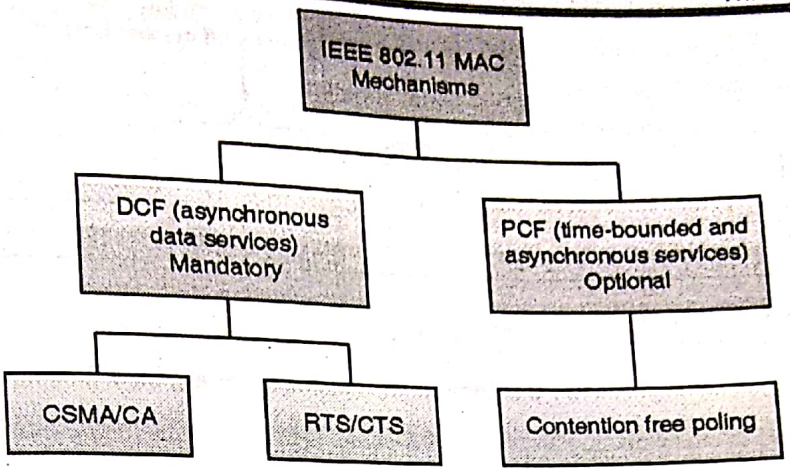


Fig. 4.2.11 : MAC mechanisms

Inter-Frame Spacing

- IEEE 802.11 offers three inter-frame spacing (IFS) between transmissions of frame.
- After completion of transmission, each station having a packet waits for one of the three IFS periods depending on the type of the packet.

(i) Short Inter-Frame Spacing (SIFS)

- This is the shortest waiting time for medium access.
- The higher priority packets such as short control messages, acknowledgement of data packets or polling responses have to wait for SIFS before medium access.

(ii) Distributed Coordinating Function IFS (DIFS)

- This denotes the longest waiting time and has the lowest priority for medium access.
- Lowest priority packets such as payload packets (packets containing data) have to wait for DIFS before the medium access.
- DIFS is a SIFS plus two slot times.

(iii) Point Coordinating Function IFS (PIFS)

- This is the waiting time between DIFS and SIFS.
- It is used by the access point.
- Before polling other nodes, the access point has to wait for PIFS time for medium access.

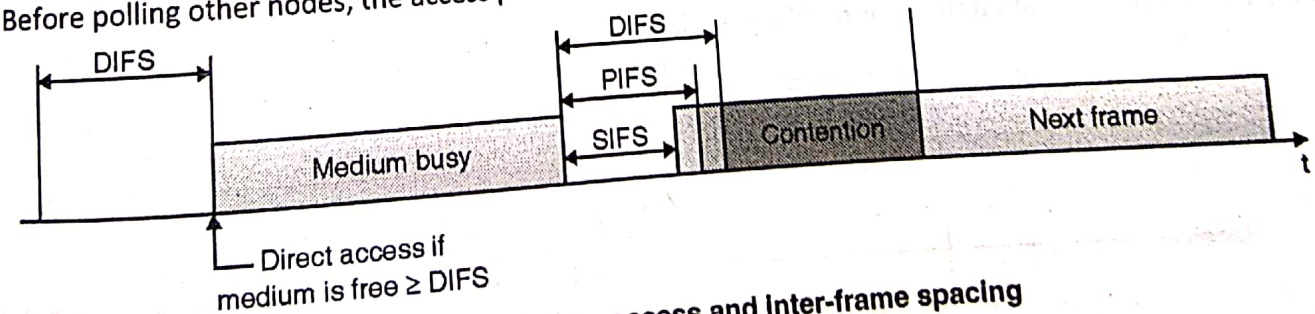


Fig. 4.2.12 : Medium access and inter-frame spacing

Basic DFWMAC-DCF using CSMA/CA

- It is a mandatory method and is used for only asynchronous data services.
- It is based on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).

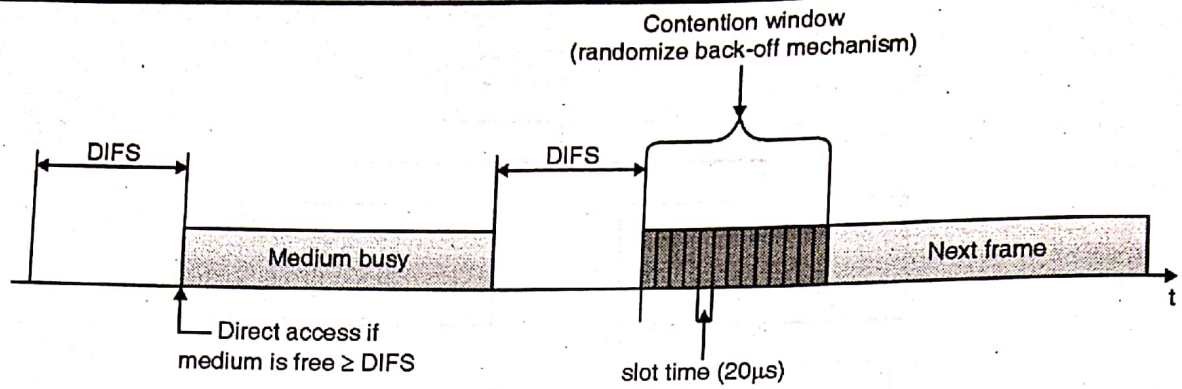


Fig. 4.2.13 : Contention window and waiting time

It works as follows

- If the medium is idle for at least DIFS time duration a node can access the medium.
- Node checks whether the medium is free or not with the help of the CCA (Clear Channel Assessment signal) in the PHY layer.
- If the medium is busy, then all the nodes wanting to access the medium wait until the medium becomes free.
- Once the medium is free, all the competing nodes wait for DIFS time period. After waiting for a DIFS time, competing nodes enter in **contention phase.**
- Now each node chooses a random back-off time within the contention window and does not try to access the medium for this random amount of time.
- Once the randomized waiting time for a node is over, the node continues to sense the medium. As soon as the node senses the channel is busy, it has lost this cycle and has to wait for a next chance i.e. until the medium becomes idle for at least DIFS time.
- But if the randomized additional waiting time for a node is over and the medium is still idle, the node can access the medium immediately and can start transferring data.
- To provide fair access mechanism, IEEE 802.11 adds a **back off timer.**
- Each station now chooses a back-off timer in the range of contention window.
- If a station does not get access to the medium in the first cycle, the back-off timer **is not cleared, instead it is just paused.**
- In the next contention cycle, the node does not choose a new random back-off time, the timer continues from where it was paused.
- Thus the stations that have waited for a longer time access the medium first.
- Fig. 4.2.14 shows unicast data transfer using DFWMAC-DCF.

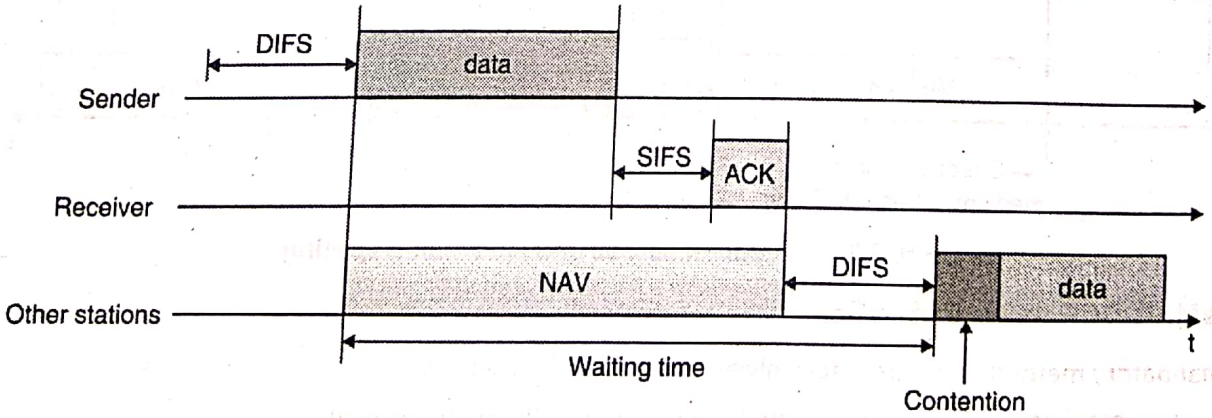


Fig. 4.2.14 : IEEE 802.11 unicast data transfer

- As shown in Fig. 4.2.14, the sender accesses the medium after waiting for DIFS time and transmits data.
- The other stations read the MAC frame and detect from the ***duration field*** how long the channel will be busy. Therefore they can set their NAV (Net allocation vector) for the appropriate time period.
- After waiting for SIFS the receiver acknowledges if the packet was received correctly.
- If no ACK is returned by the sender, after the timer expires, the sender retransmits that packet.
- The contention window starts after NAV + DIFS period. All other stations competing for the channel now choose a randomized back off timer after which they sense a channel.
- The station with the shortest back off time finds the channel idle and starts to transmit data.

DFWMAC-DCF with RTS/CTS extension

- To avoid hidden terminal problem, IEEE 802.11 defines RTS/CTS protocols. It works as follows.
- The process of unicast data transfer using RTS/CTS is illustrated in Fig. 4.2.15.
- If a terminal is willing to send data, after waiting for DIFS (plus a random backoff time if the medium was busy), it sends a short RTS control packet.
- The RTS packet contains the source address, destination address and the duration of the whole data transmission including the acknowledgement.
- All other nodes receiving RTS packets set their net allocation vector (NAV). NAV is set in accordance with the duration field specified in the RTS packet. These stations will not try to access the medium for this duration.
- The destination station responds to this packet by sending CTS control packet after an SIFS period.
- This CTS packet contains the duration field again and all stations receiving the CTS from the receiver of the data transmission set their NAV

> **Note :** This is needed because the set of stations receiving RTS can be different from the set of stations receiving CTS, thus separate NAV has to be set by the receivers of RTS and the receivers of CTS).

- The source terminal receives the CTS and sends data after waiting for SIFS.
- The destination terminal sends ACK after another SIFS.
- After completion of transmission, NAV of each station terminated and channel is available for other users.

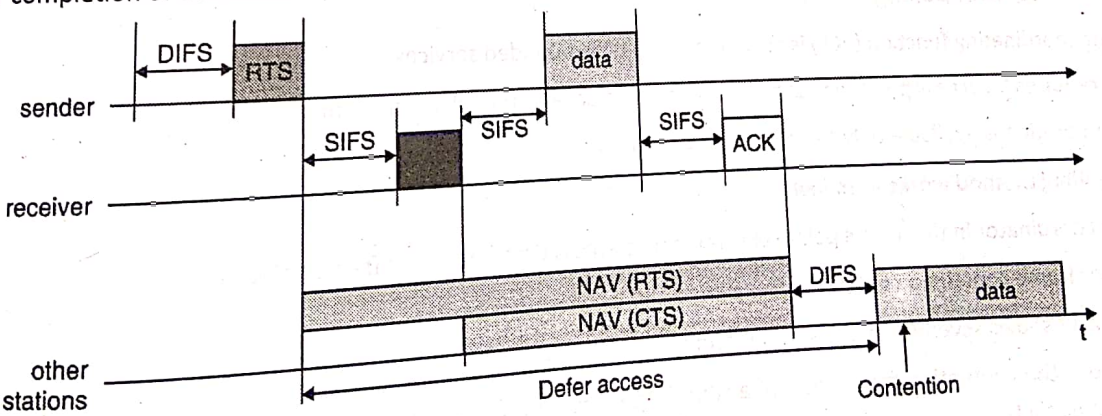


Fig. 4.2.15 : Implementation of RTS/CTS mechanisms in the IEEE 802.11

Fragmented mode of DFWMAC-DCF with RTS/CTS

- If we fragment the large frames (packets) into shorter frames then the **bit error rate** will remain the same but now short frames are destroyed and hence the **frame error rate** (rate of error per frame) decreases. Fig. 4.2.16 shows the fragmentation mode of RTS/CTS.

- Here the data frame is fragmented into smaller frames.
- Sender sends an RTS after waiting DIFS time. This RTS includes the duration for the transmission of the first fragment and the corresponding ack.
- Other stations receiving this RTS sets their NAV (for RTS) according to the duration specified in RTS.

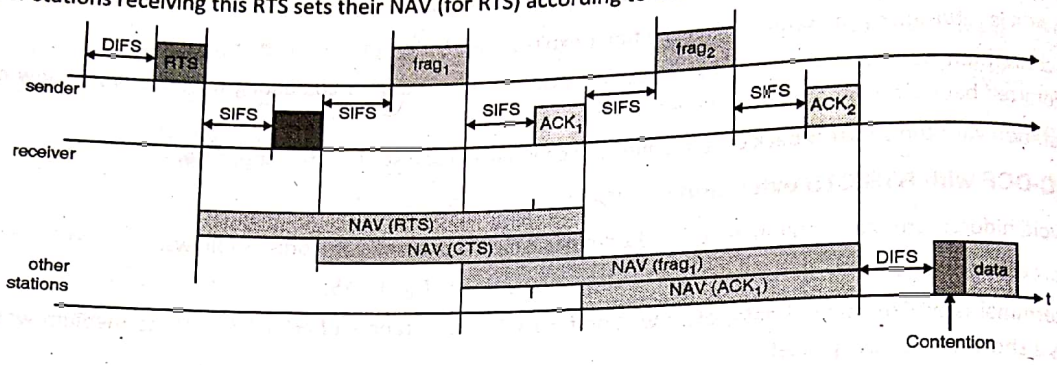


Fig. 4.2.16 : IEEE 802.11 fragmentations of data

- The receiver now answers with CTS, again including duration field.
- Receivers of CTS set their NAV (for CTS) according to the duration field.
- The sender can now send the first fragment (frag1) after waiting for SIFS time.
- The fragment 1 includes duration value. This duration field reserves the medium for the transmission of the following fragments (that is for second fragment and its ack).
- Again, all other stations receive this reservation and adjust their NAV (for frag1) accordingly.
- The receiver of frag1 sends ack for frag1 after waiting for SIFS time. This ack includes reservation for the next fragment.
- Other stations receiving this ack set their NAV for (ack1) accordingly.
- If the fragment is the last fragment then it does not reserve the medium (Duration field is empty) and the medium is now free for other stations.

DFWMAC-PCF with polling

- Point coordinating function (PCF) is used to provide time-bounded services.
- PCF requires an access point that controls the medium access and polls a single node.
- PCF operation is available only for infrastructure networks.

The PCF polling method works as follows

- Point coordinator in the access point splits the entire access time into super frame periods.
- A super frame contains a ***contention free period*** and a ***contention period***.
- Fig. 4.2.17 shows several wireless stations and their NAV.
- At time t_0 the contention-free period of a superframe should theoretically start but because the medium is busy it is postponed till t_1.
- After waiting for a PIFS time, the point coordinator (AP) sends D_1 data to poll first station. This station can reply once after SIFS.
- After waiting for SIFS time, the point coordinator sends D_2 data to poll second station. This station may answer by sending U_2 data after SIFS.

- The point coordinator now sends D_3 to poll third station. This time third station has nothing to send. The point coordinator will not receive anything after SIFS time.
- Now, the point coordinator can poll other stations after waiting PIFS time.
- The point coordinator can send end marker (CF_{end}) that indicates the end of contention-free period and the start of contention period.
- The contention period can be used for BASIC- DFWMAC or DWFMAC with RTS/CTS.
- Once the contention period is over (after t_3) the next superframe starts and the above process starts again.

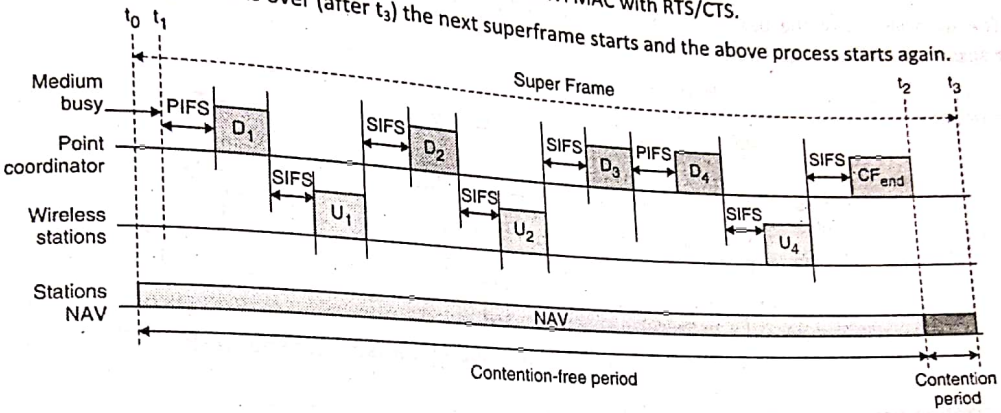


Fig. 4.2.17 : DFWMAC-PCF with polling

4.2.5 MAC Management

Following are the responsibilities of **MAC Management sub layer :**

(a) Synchronization

(b) Power Management

(c) Association/Reassociation

(d) MAC Management Information Base(MAC MIB)

4.2.5(a) Synchronization in IEEE 802.11

MU – May 15

Q. Explain synchronization in 802.11 MAC management layer for both infrastructure as well Ad-hoc WLANs. **(May 15, 10 Marks)**

- Each node of an IEEE 802.11 network maintains an internal clock.
- To synchronize the clocks of all nodes, IEEE 802.11 specifies a timing synchronization function (TSF).
- These synchronized clocks are needed for :
  - Power management
  - Coordination of the PCF
  - Synchronization in FHSS hopping sequence.

Synchronization process for infrastructure based networks

- In infrastructure based networks, an access point coordinates the synchronization process.

- The AP transmits a special frame called **beacon** periodically.
- A beacon frame consists of a time stamp and other management information used for power management and roaming.
- Other wireless nodes adjust their local clocks with beacon time stamp.
- The node is not required to hear every beacon to stay synchronized, however from time to time its clock should be adjusted.
- The transmission of the beacon is not always periodic. If the medium is busy, the access point postponed the transmission of the beacon frame.

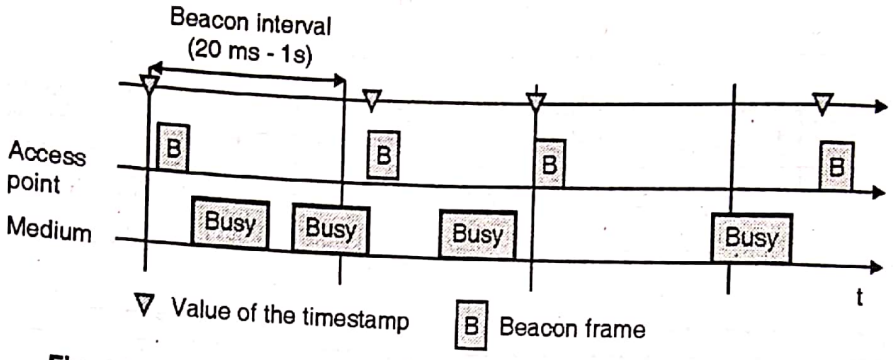


Fig. 4.2.18 : Beacon transmission in 802.11 infrastructure network

Synchronization process for ad-hoc networks

- As there is no access point in ad hoc network, each node within the network is responsible for the synchronization process.
- After each beacon interval, all stations choose random back-off time.
- Only one station whose random delay time is less becomes the winner and can send the beacon frame. All other stations adjust their local clock accordingly.

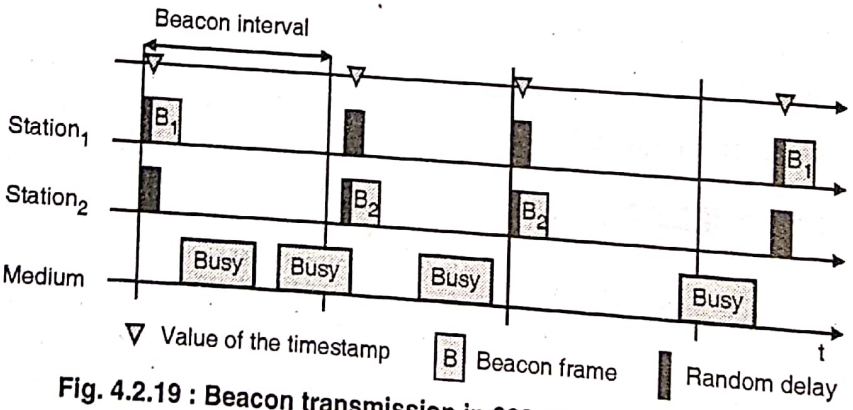


Fig. 4.2.19 : Beacon transmission in 802.11 ad-hoc networks

4.2.5(b) Power Management in IEEE 802.11

Q. Explain how the power management is done in IEEE 802.11 infrastructure based and ad-hoc networks. **MU – May 12, Dec. 13, Dec. 17**

(May 12, Dec. 13, Dec. 17, 10 Marks)

- Since wireless devices are powered by battery; power saving is a big challenge in IEEE 802.11.
- The basic idea to save power in WLAN is to switch off the transceiver whenever it is not needed.
- Each station can be in one of the two states **(1) sleep (2) awake.**

- If a sender is willing to communicate with a power saving station (station in sleep mode) then the sender has to buffer data.
- The sleeping station awakes periodically and remains awaken for a certain period of time.
- During this time all stations announce destinations of their buffered data.
- If a station sees that it is a destination of a buffered data, then it stays awake until the transmission takes place.
- All stations should wakeup or be awake at the same time. For this, Time Synchronization Function (TSF) is used.

Power management in infrastructure based networks

- In infrastructure networks, an access point is responsible for the power management function.
- Access point buffers data packets for all sleeping stations.
- The access point transmits a Traffic Indication Map (TIM) with a beacon frame. TIM consists of a list of destinations of buffered data.
- Additionally, the access point also maintains a Delivery Traffic Indication Map (DTIM) interval. DTIM is used for sending broadcast/multicast frames.
- The DTIM interval is always a multiple of TIM intervals.

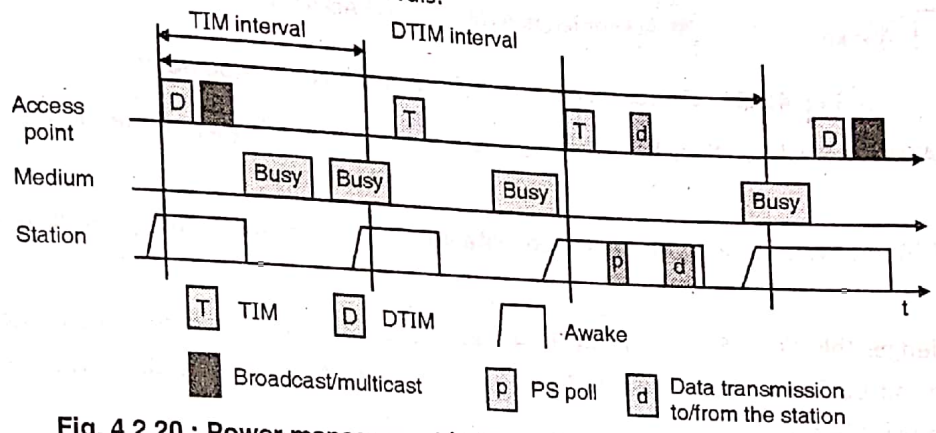


Fig. 4.2.20 : Power management in IEEE 802.11 infrastructure networks

- All stations wake up prior to an expected TIM and DTIM.
- As shown in Fig. 4.2.20, at the start of the DTIM interval, the access point has to transmit a broadcast frame. Therefore, the station stays awake until it receives that a broadcast frame.
- After receiving the broadcast frame, a station goes back to the sleep mode.
- The station wakes up again before the next TIM transmission. But the access point delays the transmission of the next TIM due to the busy medium, so the station stays awake.
- This time, the access point has nothing to send. Hence the station goes back to sleep after some time.
- At the next TIM, the access point indicates that the station is the destination of buffered data.
- The destination station replies by sending **PS** (power saving) **Poll.** And the station stays awake to receive that data.
- After receiving data, the station sends an acknowledgement or may send some data and goes back to sleep.
- In the next DTIM, the access point has more broadcast data to send and the station has to awake to receive that data.

Power management in ad-hoc networks

- In ad-hoc networks, power management is more difficult than in infrastructure networks because there is no access point to buffer data for power saving stations.
- Here, each station buffers data that it wants to send to power saving stations.
- In ad-hoc networks, all stations announce a list of buffered frame during a period when they are all awake.

- All stations announce destinations for which packets are buffered using ATIM (Ad-hoc traffic indication map) during the ATIM interval.
- As shown in Fig. 4.2.21 all stations awake at the same time and stay awake for ATIM interval.

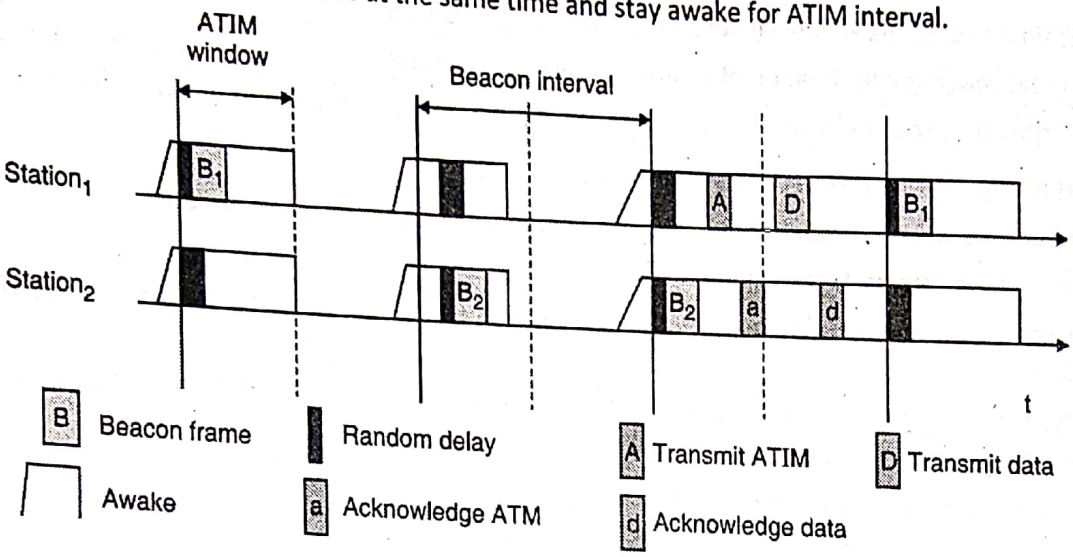


Fig. 4.2.21 : Power management in IEEE 802.11 ad-hoc networks

- In the first two ATIM intervals, stations have nothing to send, hence, stations stay awake for ATIM interval and later go back to sleep.

  In the third ATIM interval, station$_1$ has buffered data for station$_2$ hence station$_1$ sends ATIM (Shown as **A** in Fig. 4.2.21).
- Station$_2$ acknowledges this ATIM (Shown as **d** in Fig. 4.2.21) and stays awake for transmission. After the ATIM window, Station$_1$ can transmit buffered data (Shown as **D** in Fig. 4.2.21) and station$_2$ sends acknowledgement (shown as **d** in Fig. 4.2.21) or data (if it has) in reply.

4.2.5(c) Association/ Reassociation

1. Association

- Once authentication is completed, stations can associate with an access point (or reassociate with a new access point) to gain full access to the network.
- Association allows the distribution system to track the location of each mobile station.
- The basic procedure of association is shown in Fig 4.2.22.

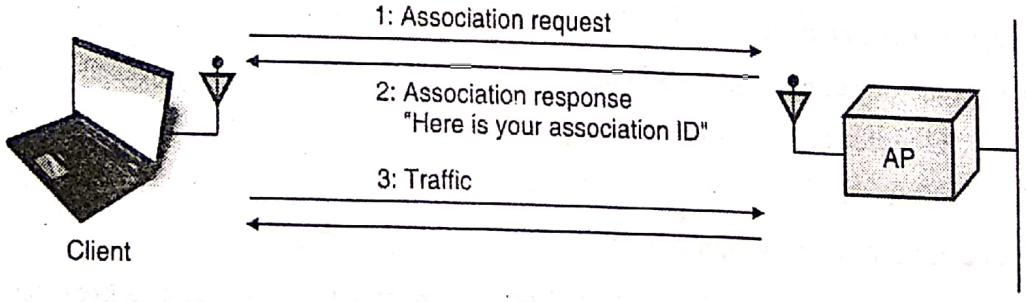


Fig. 4.2.22 : Association

Association Procedure :

(i) Once a mobile station has authenticated to an access point, it can issue an Association Request frame.

(ii) The access point then processes the association request.

(a) When the association request is granted, the access point responds with a status code of 0 (successful) and the Association ID (AID). The AID is a numerical identifier used to logically identify the mobile station to which buffered frames need to be delivered.

(b) Unsuccessful association requests include only a status code, and the procedure ends.

2. Reassociation

Reassociation is the process of moving an association from an old access point to a new one.

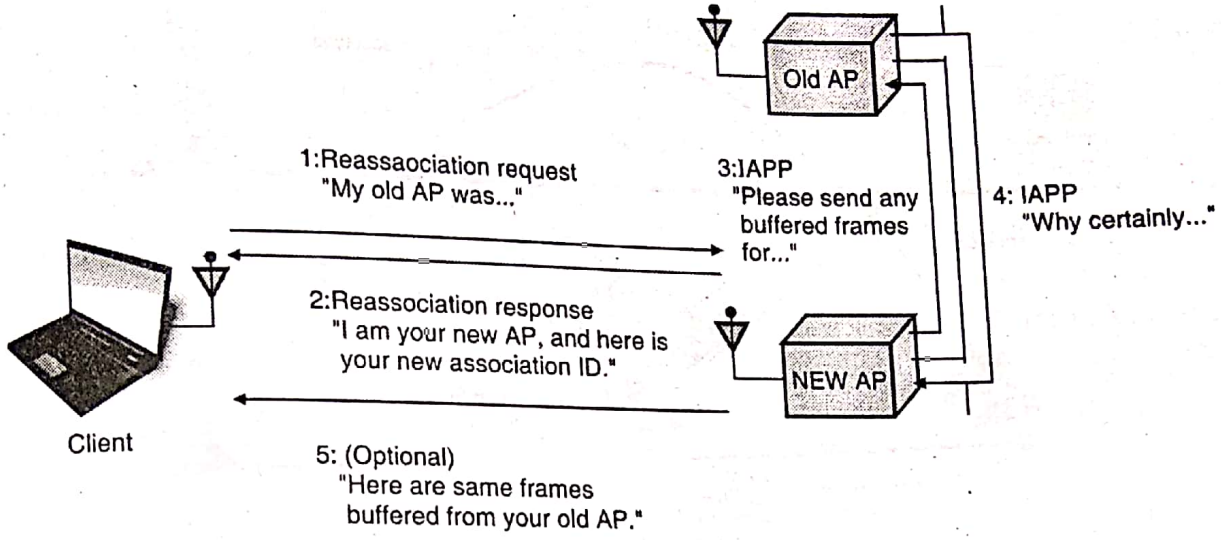


Fig. 4.2.23 : Reassociation procedure

Reassociation Procedure :

- The station monitors the quality of the signal it receives from that access point, as well as the signal quality from other access points in the same ESS.
- When the mobile station detects that it's receiving better signal from other access point, it initiates the reassociation procedure.

Fig. 4.2.23 depicts the following steps :

1. The mobile station issues a Reassociation Request to the new access point.
2. The new access point must communicate with the old access point to verify that the old access point authenticated the station. If the verification fails then the new access point responds with a Deauthentication frame and ends the procedure.
3. The access point processes the Reassociation Request. Processing Reassociation Requests is similar to processing Association Requests :
   (a) If the Reassociation Request is granted, the access point responds with a Status Code of 0 (successful) and the AID.
   (b) Unsuccessful Reassociation Requests include just a Status Code, and the procedure ends.
4. The new access point contacts the old access point to finish the reassociation procedure. This communication is part of the IAPP.
5. The old access point sends any buffered frames for the mobile station to the new access point.

6. The old access point terminates its association with the mobile station.
7. The new access point begins processing frames for the mobile station. When it receives a frame destined for the mobile station.

Roaming/ Scanning

When a mobile station moves from one access point to another access point then it has to associate with new access point for uninterrupted service, this moving between access points called roaming (Handoff). The steps for roaming handoff between access points are as follows (Refer Fig. 4.2.24) :

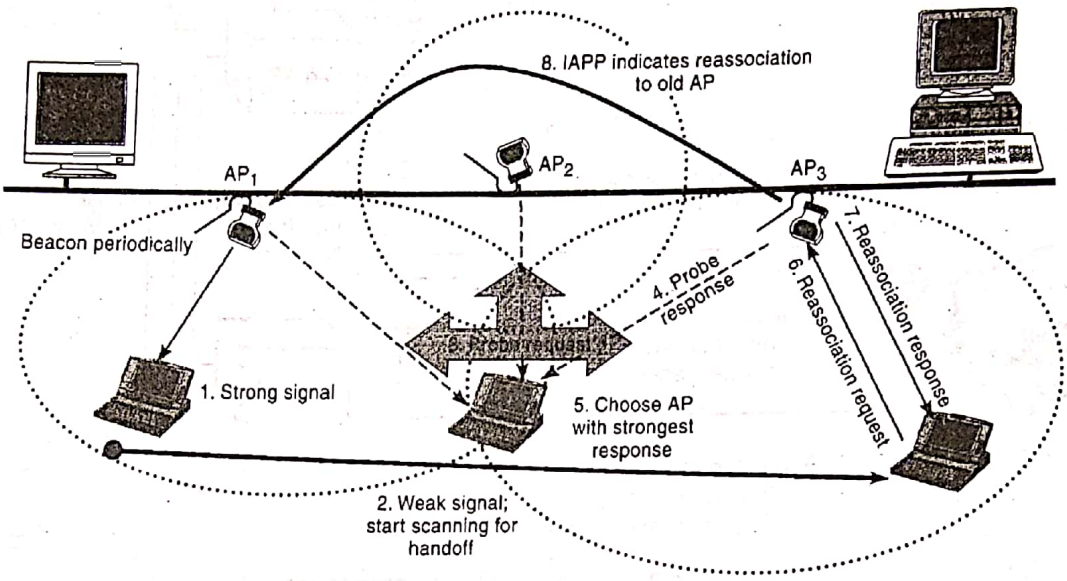


Fig. 4.2.24 : Roaming in IEEE 802.11 WLAN

- When station moves from one BSS to another its link quality from the access point AP_1 becomes poor. The station then starts scanning for another access point.
- Scanning involves search for another BSS or setting up new BSS in the case of ad-hoc networks. Scanning may be active or passive. In **Active scanning** station sends a **probe** on each channel and wait for a response. In **Passive scanning** the station listen to the medium i.e. station receives beacon signal of another network. Probe and beacon contains the necessary information to join the new access point.
- The station then select the best access point AP_3 with the strongest probe/ beacon signal strength, and send ***reassociation request*** to the selected access point.
- The new access point answers with **reassociation response.** If the response is successful, the station has roamed to the new access point.
- The new access point used IAPP (Inter Access Point Protocol) to inform to the old access point AP_1 about the change of access point.

4.2.5(d) MAC Management Information Base (MAC-MIB)

IEEE 802.11 Management Information Base (MIB) is a database used for managing the entities in a Wireless LAN. It can be construed as an SNMP Managed object with several configuration controls, option selectors, counters, and status indicators. These different attributes permit an external management agent to determine the status and configuration of an IEEE 802.11 station. The MIB in a station comprises separate sections for MAC and PHY.

4.2.6 IEEE 802.11a

- It operates at **5 GHz** frequency band.
- It offers maximum data rate of **54 Mbits/s.**
- Uses **OFDM** (Orthogonal FDM) modulation scheme for achieving such a high data rate.
- Transmission range is 100m outdoor, 10m indoor.
- Here too, all the MAC schemes and management procedures are same as that of the original IEEE 802.11.
- The heart of the system is its modulation schemes and coding schemes.
- To offer high data rate, the system uses **52 sub carriers** that are modulated using various modulation schemes like BPSK, QPSK, 16-QAM and 64-QAM.
- To mitigate transmission errors, it uses **FEC** (Forward Error Correction coding) using coding rate of 1/2, 2/3 or 3/4.
- Using various combination of modulation (BPSK, QPSK etc.) and coding schemes it achieves various data rates such as 6, 9, 12, 18, 24, 36, 48 and 54 Mbits/s.

Usage of OFDM in IEEE802.11a

- The basic idea of OFDM is the reduction of the symbol rate by distributing bits over numerous subcarriers.
- IEEE 802.11a uses fixed symbol rate of 250,000 symbols per second independent of the data rate.

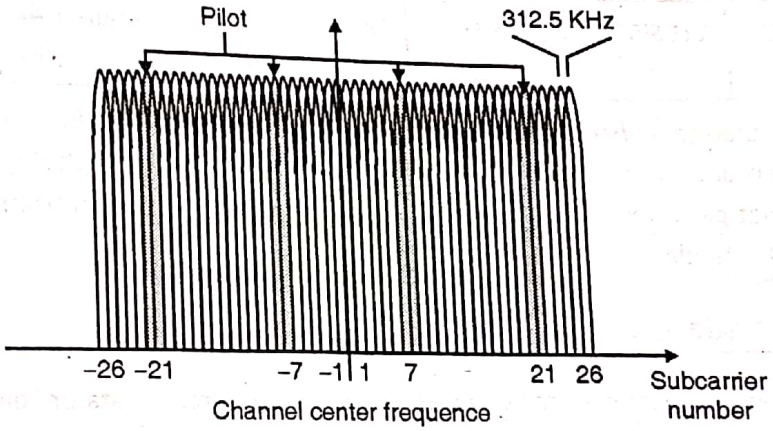


Fig. 4.2.25 : Usage of OFDM in IEEE 802.11a

- Fig. 4.2.25 shows 52 subcarriers equally spaced around a centre frequency. The spacing between the subcarriers is 312.5 KHz.
- The center frequency itself is not used as a sub carrier. Subcarriers numbered -21,-7, 7, 21 are used for pilot signals to make the signal selection robust against frequency offset.
- Compared to IEEE 802.11b that operates in 2.4 GHz the IEEE802.11a offers higher data rate and more coverage, however shading at 5GHz is much more severe compared to 2.4 GHz.

4.2.7 802.11b

- Unlike IEEE 802.11a, IEEE 802.11b operates at 2.4 GHz.
- It provides raw data rates up to 11 Mbps.
- It provides a wireless range of roughly 35 meters indoors and 140 meters outdoors.
- It uses the CSMA/CA technique.
- The RF signal format used for 802.11b is CCK or complementary Code Keying.

- IEEE 802.11b supports Adaptive Rate selection. The system monitors the signal quality. If the signal falls or interference levels rise, then system adopt a slower data rate with more error correction. The system will first fall back to a rate of 5.5 Mbps, then 2, and finally 1 Mbps. This scheme is known as Adaptive Rate Selection (ARS).

4.2.8 Comparison of Various IEEE 802.11x Standards

MU – Dec. 15

Q. Compare various IEEE 802.11x standards. (Dec. 15, 10 Marks)

Parameters	IEEE 802.11	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n
Operates at	2.4GHz	5GHz	2.4GHz	2.4 GHz	5 GHz or 2.4 GHz
Maximum data rate	2 Mbps	54 Mbps	11 Mbps	54 Mbps	300 Mbps
Modulation	DSSS, FHSS	OFDM	DSSS or CCK	DSSS or CCK or OFDM	DSSS or CCK or OFDM
Channel width	20 MHz	20 MHz	20 MHz	20 MHz	20 MHz or 40 MHz
Typical range	66 feet	75 feet	100 feet	150 feet	150 feet
Antenna configuration	1x1 SISO	1x1 SISO	1x1 SISO	1x1 SISO(Single Input-Single Output)	4x4 MIMO (Multiple Input-Multiple Output)

IEEE 802.11 is mainly designed for enhanced security purposes. It addresses two main weaknesses of wireless security networks which are encryption and authentication. Encryption is accomplished by replacing WEP's original PRNG RC4 algorithm by stronger cipher that performs three steps on every block of data. The authentication and key management is accomplished by the IEEE 802.1x standard.

4.3 Wi-Fi Security Standards

- Since wireless networks transmit data over radio waves, it is easy to intercept data or "eavesdrop" on wireless data transmissions.
- Several Wi-Fi security algorithms have been developed since the inception of Wi-Fi.
- The wireless security protocols prevent unwanted parties from connecting to your wireless network and also encrypt your private data sent over the airwaves.
- Different types of wireless security protocols have been discussed below.

4.3.1 WEP – Wired Equivalent Privacy

- WEP stands for 'Wired Equivalent Privacy'.
- WEP is specified by IEEE 802.11 for encryption and authentication of Wi-Fi networks.
- It operates at physical and data link layer.
- The goal of WEP is to make wireless networks as secure as wired networks.
- WEP is having two main parts. Authentication and Encryption.

(i) WEP Authentication

- Fig. 4.3.1 shows an example of WEP authentication:

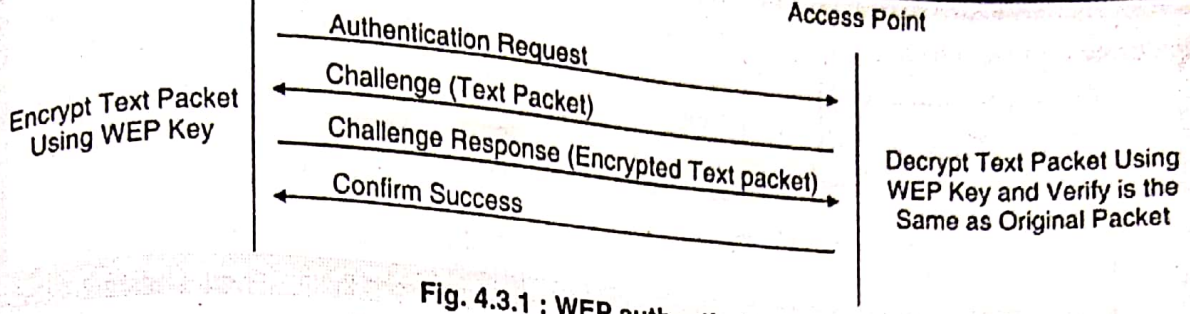


Fig. 4.3.1 : WEP authentication

- First a requesting station sends an Authentication Request to the access point (AP).
- On receiving the request, the AP, replies with a 128 byte random challenge text generated by WEP algorithm.
- The requesting node then copies the text into the authentication frame and encrypts it with a shared key , and then sends the frame back to the AP.
- The AP then will decrypt the value of the challenging text using the same shared key and compare it to the challenging text sent earlier.
- If match occurs, the AP will reply with a positive authentication indicating a successful authentication.
- If there is not a match, the AP will send back a negative authentication.

(ii) WEP Encryption

Encryption process

- WEP uses RC4 encryption which is a symmetric stream cipher to provide confidentiality.
- The 40-bit secret key is connected with a 24-bit Initialization vector (IV) resulting in a total 64 –bit key(shown as a seed in Fig. 4.3.2).
- The resulting key (seed) is the input for the Pseudo Random Number Generator (PRNG). The PRNG (RC4) outputs a pseudo random key sequence based on the input key.
- The resulting sequence is used to encrypt the data by doing a bitwise XOR.

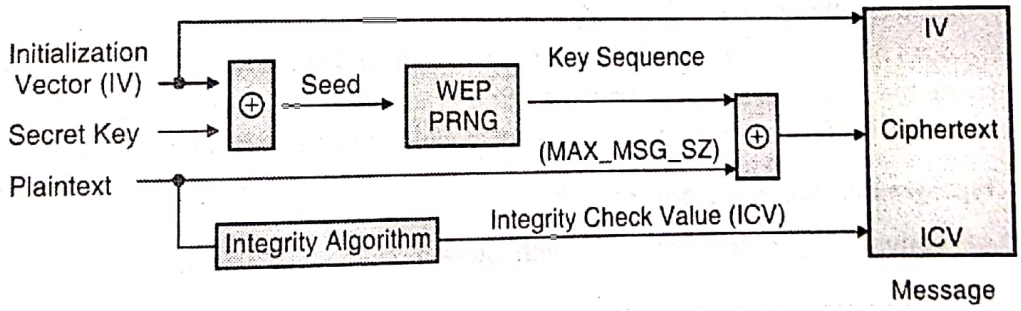


Fig. 4.3.2 : WEP Encryption

- The result is encrypted bytes equal in length to the number of data bytes that are to be transmitted in the expanded data plus four bytes. This is because the key sequence is used to protect the 32-bit Integrity Check Value(ICV) as well as the data.
- Fig. 4.3.2 shows the encryption algorithm and Fig. 4.3.3 shows the decryption algorithm.
- To prevent unauthorized data modification an integrity algorithm, CRC-32 operates on the plain text to produce ICV.
- The output of the whole process is a message containing three parts: the resulting ciphertext, the IV, and the ICV.

Decryption process

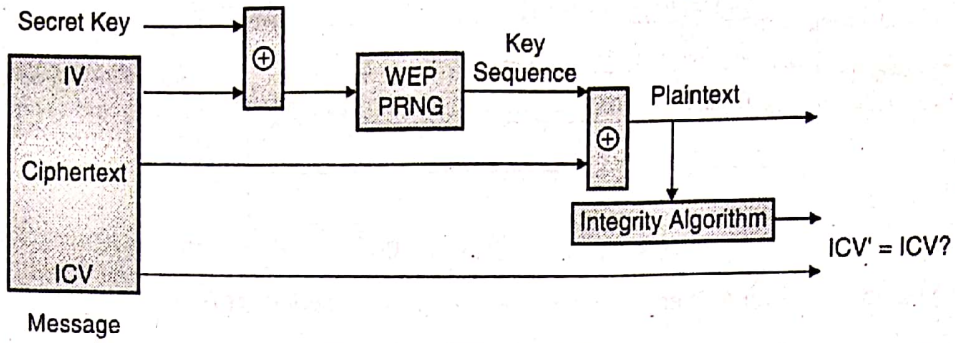


Fig. 4.3.3 : WEP Decryption

- The incoming message has three parts: Ciphertext, IV and ICV.
- The IV of the incoming message is used to generate the key sequence to decrypt the incoming message.
- Combining the ciphertext with the proper key sequence will give the original plaintext and ICV.
- The decryption is verified by performing integrity check algorithm on the recovered plain text and comparing the output of the ICV' (Calculated ICV) to the ICV submitted with the message. If calculated ICV (ICV') is not same as ICV, the received message is in error.

WEP vulnerabilities

Although WEP attempts to achieve wired equivalent security, there are still many weaknesses in WEP which may be used by the malicious user to compromise the security of WLAN.

(i) The IV is too small and in clear text.

Initial Vector used in WEP is 24-bit field sent in the clear text portion of a message. This 24-bit string, used to initialize the key stream generated by the RC4 algorithm, is a relatively small field when used for cryptographic purposes.

(ii) The IV is static.

The same IV is used to produce the key every time. Reuse of the same IV may produce identical key streams and since IV is short, it guarantees that those streams will repeat after a relatively short time.

(iii) The IV makes the key stream vulnerable.

The 802.11 standard does not specify how the IVs are set or changed, and individual wireless adapters from the same vendor may all generate the same IV sequences, or some wireless adapters may possibly use a constant IV. As a result, hackers can record network traffic, determine the key stream, and use it to decrypt the cipher text.

(iv) WEP provides no cryptographic integrity protection.

The combination of non-cryptographic checksums with stream ciphers is dangerous - and often introduces vulnerabilities. T

(v) WEP Uses Stream Cipher.

The basic problem with WEP is that it uses a stream-cipher known as RC4 in synchronous mode for encrypting data packets. Using the synchronous stream ciphers, the loss of a single bit of a data stream causes the loss of all data following the lost bit. Thus the stream cipher is not suitable for wireless medium where placket loss is widespread.

4.3.2 WPA

- WPA stands for "Wi-Fi Protected Access".
- WPA was developed by the Wi-Fi Alliance to provide better user authentication than Wired Equivalent Privacy (WEP),
- One major improvement in WPA over WEP is the Temporal Key Integrity Protocol (TKIP), which dynamically changes keys as the system is used.

- It uses RC4 stream cipher with a 128 bit key and a 48 bit IV. The longer key and IV together defeat the key recovery attacks on WEP.
- In addition to authentication and encryption, WPA also provides vastly improved payload integrity.
- The cyclic redundancy check (CRC) used in WEP is insecure; it is possible to alter the payload and update the message CRC without knowing the WEP key.
- WPA uses a solution called Michael, which is a Message Integrity Check (MIC), to the checksum being corrupted issue. WPA uses a 32 bit Integrity Check Value (ICV). This is inserted after payload and before IV. The MIC includes a frame counter, which helps to prevent replay attacks.

WPA Modes

WPA supports two modes of operation.

1. **Pre-Shared Key Mode or Personal Mode**

   This mode is used for personal use. The preshared mode does not require authentication server. It utilizes a shared key that is communicated to both sides (AP and client) before establishing a wireless connection; this key is then used to secure the traffic.

2. **Enterprise Mode**

   Enterprise Mode requires an authentication server. It uses more stringent 802.1x authentication with the Extensible Authentication Protocol (EAP). It Uses RADIUS protocols for authentication and key distribution. In this mode, the user credentials are managed centrally.

WPA2 vs. WPA and WEP

- Among all three wireless LAN security protocols, WEP is the least secure which provides security equal to that of a wired connection.
- WEP broadcasts messages using radio waves and is much easier to crack. This is because it uses the same encryption for every data packet. If enough data is analyzed by an eavesdropper, the key can be easily found with automated software.
- WPA improves on WEP by using the TKIP encryption scheme to scramble the encryption key and verify that it hasn't been altered during the data transfer.
- Further, WPA2 improves the security of a network by using stronger encryption method called AES.

4.3.3 Wireless LAN threats

There are a number of threats that exist to wireless LANS, these include:

- Rogue Access Points/Ad-Hoc Networks
- Evil Twin APs
- Denial of Service
- Configuration Problems also called Mis-Configurations or Incomplete Configurations
- Passive Capturing
- Misbehaving Clients

1. **Rogue Access Points/Ad-Hoc Networks**
   - One way that is the attackers target wireless LANs is by setting up a rogue access point.
   - A rogue access point (AP) is a wireless AP that has been installed on a secured network without any authorization from the network administrator.
   - The idea is to 'fool' some of the legitimate devices and to make them connect to the rogue access point.

2. Evil Twin Aps

- In this type of attack, the fraudulent AP advertises the same network name (SSID) as a legitimate WLAN, causing nearby Wi-Fi clients to connect to them.
- The only effective defense against Evil Twins is server authentication from 802.1X.

3. Denial of Service

- This is the most common and simplest attack. It can cripple or disable a wireless network by limiting the access to the services.
- This can be done by simply sending a large amount of traffic at a specific target.
- Here the amount of traffic generated to affect a target device is much higher than the capabilities of a target machine.
- A denial of service attack can also be used in conjunction with a rogue access point. For example, a rogue access point could be setup in a channel that is not used by the legitimate access point. Then the denial of service attack could be launched at the channel currently being used causing endpoint devices to try to re-associate onto a different channel which is used by the rogue access point.

4. Configuration Problems

- Simple configuration problems are often the cause of many vulnerabilities. A novice user can set up one of these devices quickly and gain access. However, they also open up their network to external use without further configuration.
- Other issues with configuration include weak passphrases, weak security algorithm deployments (i.e. WEP vs WPA vs WPA2), and default SSID usage.

5. Passive Capturing

- Passive capturing is performed by simply getting within the range of a target wireless LAN and then listening and capturing data.
- This information can be used for a number of things including attempting to break existing security settings and analyzing non-secured traffic.
- It is almost impossible to really prevent this type of attack because of the nature of a wireless network; what can be done is to implement high security standards using complex parameters.

6. Misbehaving Clients

- Sometimes clients form unauthorized Wi-Fi connections accidentally or intentionally. By doing this, they put themselves and corporate data at risk.
- Some enterprises use Group Policy Objects to configure authorized Wi-Fi connections and prevent end-user changes. Others use host-resident agents to monitor Wi-Fi client activity and disconnect high-risk connections.

4.3.4 Securing Wireless Network

The following are some of the ways by which you can secure wireless network.

1. Use an inconspicuous network name (SSID)

- The Service Set Identifier (SSID) is one of the most basic Wi-Fi network settings. Avoid using too common SSID, like "wireless" or the vendor's default name.
- This can make it easier for someone to crack the personal mode of WPA security.

2. **Use Enterprise WPA2 with 802.1X authentication**
   - Use enterprise mode of Wi-Fi security, because it authenticates every user individually - Everyone can have their own Wi-Fi username and password. So if a laptop or mobile device is lost or stolen, or an employee leaves the company, all you have to do is change or revoke that particular user's log-ins.
   - In contrast, in personal mode, all users share the same Wi-FI password, so when devices go missing or employees leave you have to change the password on every single device.
   - Another advantage of enterprise mode is that every user is assigned his or her own encryption key. That means users can only decrypt data traffic for their own connection — no snooping on anyone else's wireless traffic.

3. **Use firewalls to secure your Wi-fi network**
   - Use A hardware firewall. A hardware firewall does the same thing as a software one, but it adds one extra layer of security.
   - The best part about hardware firewalls is that most of the best wireless routers have a built-in firewall that should protect your network from potential cyber attacks.
   - If your router doesn't have one, you can install a good firewall device to your router in order to protect your system from malicious hacking attempts against your home network.

4. **Restrict access**

   Only allow authorized users to access your network. Each piece of hardware connected to a network has a media access control (MAC) address. You can restrict access to your network by filtering these MAC addresses.

5. **Encrypt the data on your network**

   Use strong encryption algorithm to encrypt data. There are several encryption protocols available to provide this protection. Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and WPA2 encrypt information being transmitted between wireless routers and wireless devices. WPA2 is currently the strongest encryption.

6. **Maintain antivirus software**

   Install antivirus software and keep the virus definitions up-to-date. Many antivirus programs also have additional features that detect or protect against spyware and adware.

7. **Use file sharing with caution**

   File sharing between devices should be disabled when not needed. Allow file sharing over home or work networks, never on public networks. Create a dedicated directory for file sharing and restrict access to all other directories. Anything that is been shared should be password protected.

8. **Keep your access point software patched and up-to-date**

   The manufacturer of your wireless access point periodically release updates. Update access point software website regularly.

9. **Connect using a virtual private network**

   Many companies and organizations have a Virtual Private Network (VPN). VPNs allow employees to connect securely to their network when away from the office. VPNs encrypt connections at the sending and receiving ends and keep out traffic that is not properly encrypted.

4.4 HIPERLAN Standards

- There are two main standard families which are used for Wireless LAN :

(i) IEEE 802.11 (802.11b, 802.11a, 802.11g...)

(ii) ETSI HIPERLAN (HIPERLAN Type 1, Type 2, HiperAccess, HiperLink)

- HIPERLAN is a European (ETSI) standardization initiative for a High Performance Wireless Local Area Network.
- ETSI defined four types of HIPERLANs: HIPERLAN/1, HIPERLAN/2, HIPERACCESS and HIPERLINK.

4.4.1 HIPERLAN T-1

MU – May 12

Q. Write a short note on HIPERLAN. **(May 12, 5 Marks)**

- HIPERLAN-1 operates in the dedicated bandwidth **5.15 to 5.3 GHz** divided into 5 fixed channels.
- It supports data rate up to **23.5 Mbps** with coverage of 50m.
- HIPERLAN-1 terminals can move at the maximum speed of **1.4m/s**.
- It supports both **infrastructure based** and **ad-hoc networks**.
- It supports packet oriented structure and uses a variant of **CSMA/CA protocol**.
- Supports asynchronous as well as isochronous traffic.
- The protocol includes optional pre-session encryption and power saving mechanism.
- Fig. 4.4.1 presents the HIPERLAN-1 reference layer model (Protocol stack). Fig. 4.4.2 shows the HIPERLAN communication model.

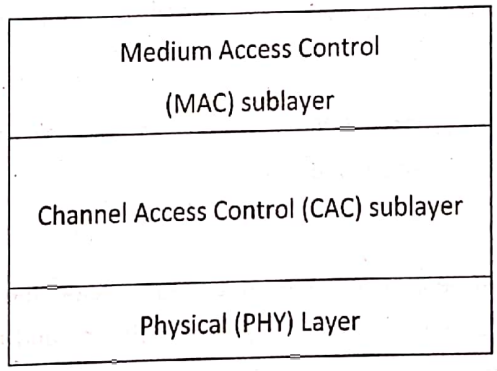


Fig. 4.4.1 : HIPERLAN -1 protocol stack

- The MAC layer receives MAC service data units (MSDU) form the higher layers through MAC service access point.
- It processes MSDU and generates HMPDU (HIPERLAN MAC Protocol Data Unit)
- This HMPDU then enters HIPERLAN CAC layer through a HIPERLAN–CAC service access point (HCSAP).
- The Channel Access Control (CAC) sub layer determines which nodes are allowed to transmit and specifies the access priorities.
- This layer offers a ***connection less service*** to the MAC sub layer.
- CAC protocol processes the HMPDU and produce HCPDU (HIPERLAN-CAC Protocol Data Unit) which finally constitute a payload of a physical data burst.

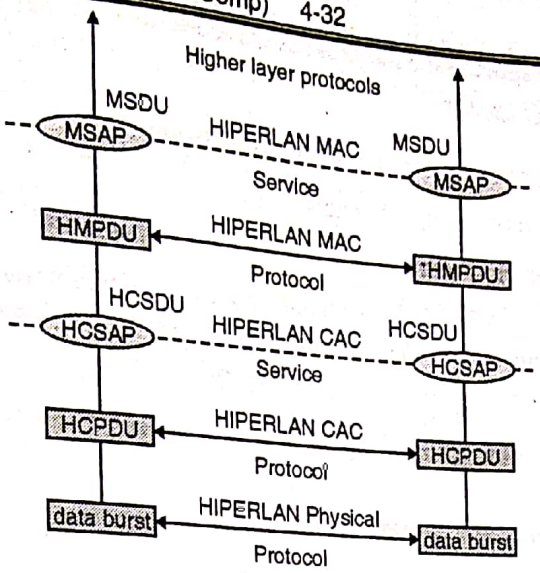


Fig. 4.4.2 : HIPERLAN Communication model

4.4.1(a) HIPERLAN-1 MAC Sublayer

MU – May 18

Q. Explain HIPERLAN 1 MAC Layer. (May 18, 10 Marks)

MAC sublayer functions are listed below.

1. MAC address mapping

- The standard defines internal address structure.
- The address of a HIPERLAN terminal contains two parts. The first part defines the network name and the second part determines the station.

2. Security

- To ensure communication security, the Encryption/Decryption algorithms are used.
- The algorithm requires an identification key and a common initialization vector for data encryption and decryption.
- The pseudorandom generator accepts the identification key and the initial vector and generates a sequence.
- The modulo-2 addition is performed on the sequence of user data and the sequence generated by the pseudorandom generator.
- Initialization vectors and identification keys can be frequently changed in order to achieve high security.

3. Addressing of MAC service access point (MSAP)

MSAP are addressed using 48 bit LAN-MAC address which are compatible to IEEE 802.x LANs.

4. Data forwarding

- The appealing feature of HIPERLAN/1 is ability to forward data packets using several relays. Relays can extend the communication on the MAC layer beyond the radio range.
- The forwarding can be of two types-point-point (unicast) or point-multipoint (multicast/broadcast).
- Each relay station maintains a routing table and a list of multipoint relays.

5. Power saving

Switch off terminals whenever they are not in use or keep in sleep mode when they don't have data to send.

4.4.1(b) HIPERLAN-1 CAC Layer

Functions of Channel Access Control (CAC) sub layer are listed below :

- Assures that terminal does not access illegal channels.
- Defines how a given channel can be accessed.
- Defines the priority scheme. It uses EY-NPMA (Elimination Yield Non-preemptive Priority Multiple Access). EY-NPMA supports both asynchronous and isochronous (voice-oriented) transmission. EY-NPMA enables network to function with few collisions.
- Provides five priority levels for QoS supports. The mapping of a QoS on a priority level is done with the help of packet life time.
- Provides hierarchical independence with EY-NPMA.

EY-NPMA

- The most important part of CAC sub layer is the Elimination Yield Preemptive Priority Multiple Access (EY- NPMA) protocol.
- It is a variant of CSMA protocol with prioritization.
- It divides the medium access of different competing nodes into three phases.

1. Prioritization 2. Contention 3. Transmission

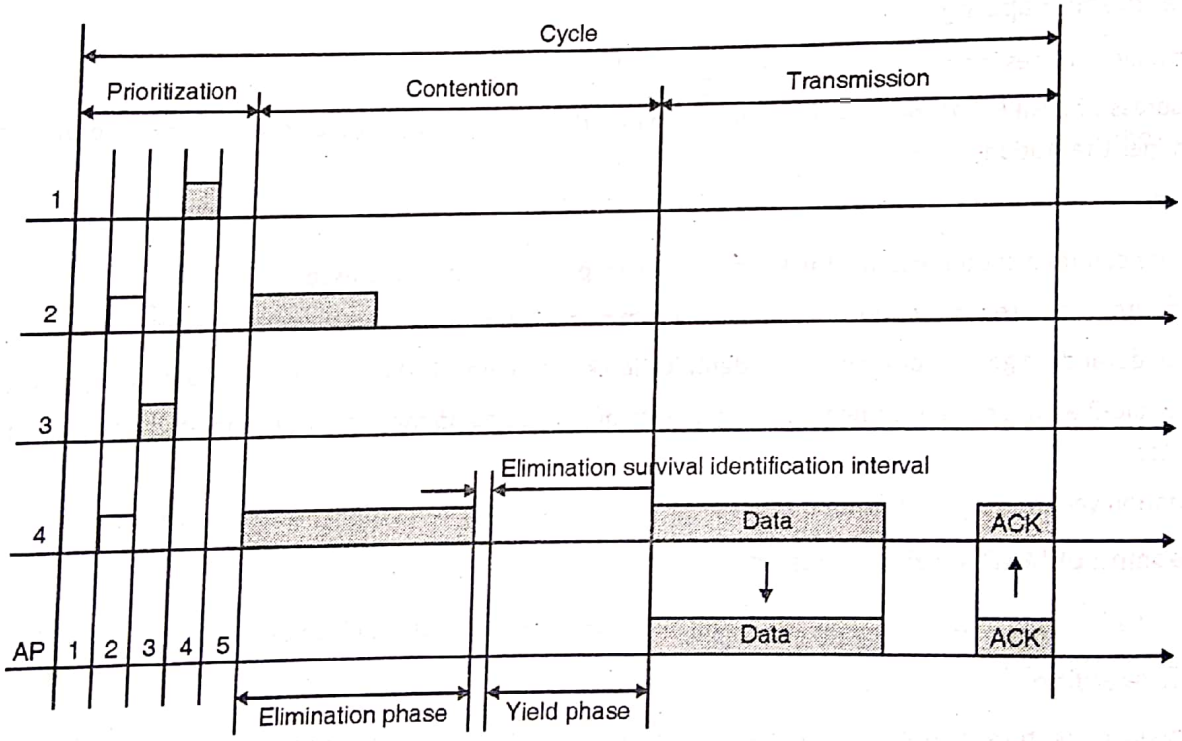


Fig. 4.4.3 : EY-NPMA protocol (Channel access cycle)

1. Prioritization

- Time is divided into channel access cycles. Each cycle starts with the channel access synchronization.
- The synchronization is followed by the prioritization phase. This phase contains five 168-bit slots starting from the slot of highest priority (p=1).
- If the terminal has the priority, *p* it senses the channel for the first (*p*-1) slots.
- If the channel remains idle, the node sends an access pattern.

- If the node finds that the channel is busy, it waits for the beginning of the next access cycle.
- More than one station can have the same priority.
- So, next contention phase is carried out to resolve contention problem.

2. **Contention**
   - This phase is further divided into two phases : Elimination phase and Yield phase.
   - The **elimination phase** is divided into 0-12 slots. Each terminal which has not been eliminated in the prioritization phase sends the elimination burst. The length of this burst is random between 0 to 12.
   - After sending an elimination burst, each station senses the channel during elimination survival verification interval.
   - A station gives up if the channel is occupied by some other station during this interval.
   - The **yield phase** contains ten 168-bit slots. Each station senses channel during *n* slots (0-9).
   - The probability that the given station senses the channel for *n* consecutive slots is 1/10.

3. **Transmission**
   - If the station does not detect any activity in the channel during listening, it immediately starts transmitting and enters transmission phase.
   - If the station has detected that the channel is busy, it has lost its cycle and waits till the beginning of the next access cycle.

4.4.1(c) HIPERLAN-1 Physical Layer

MU – May 16

Q. Explain in detail HIPERLAN-1 physical layer. (May 16, 10 Marks)

Functions of the physical layer of HIPERLAN are listed below :

- Modulation, demodulation (uses FSK,GMSK)
- Bit and frame synchronization
- Forward error correction mechanisms (uses BCH codes)
- Measurements of signal strength
- Channel sensing
- HIPERLAN-1 provides 3 mandatory and 2 optional channels according to their carrier frequencies.

(i) **Mandatory channels**
   - Channel 0: 5.1764680 GHz
   - Channel 1: 5.1999974 GHz
   - Channel 2: 5.2235268 GHz

(ii) **Optional channels**
   - Channel 3: 5.2470562 GHz
   - Channel 4: 5.2705856 GHz

- HIPERLAN-1 uses non differential Gaussian minimum Shift Keying (non differential GMSK).
- It uses adaptive equalizer called decision feedback equalizer (DFE) to remove inter symbol interference (ISI) caused due to multipath propagation.

- HIPERLAN-1 also employs BCH error correcting codes to minimize the errors at physical layer.
- This code is able to correct a single error and detect two random errors, all errors bursts not longer than 5 – bits.
- Fig. 4.4.4 presents HIPERLAN-1 data packet format used at physical layer.

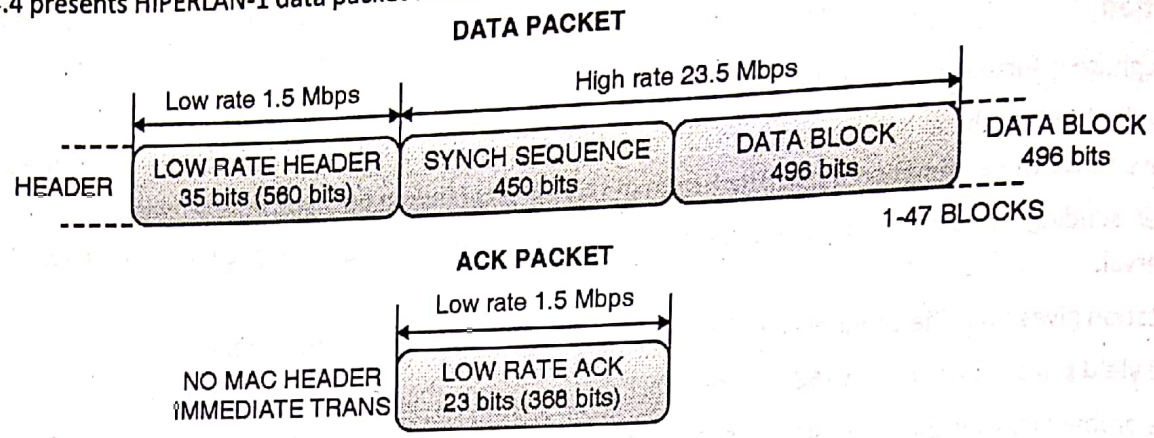


Fig. 4.4.4 : HIPERLAN-1 physical layer packet format for data and acknowledgement

4.4.2 HIPERLAN -2

MU – Dec. 18

Q. Explain HIPERLAN-2 Data link control. **(Dec. 18, 10 Marks)**

HIPERLAN2 allows interconnection in almost any type of fixed network.

Features of HIPERLAN- 2

- Operates at **5 GHz** frequency band
- Provides Connection-oriented service
- High speed transmission up to **54 Mbit/s** (same as IEEE 802.11a)
- Quality-of-Service (QoS) support
- Automatic frequency allocation
- Security support
- Mobility support
- Network and application independent
- Power saving

Reference model and configuration of HIPERLAN-2

- HIPERLAN-2 is designed to work in two configurations: business environment and home environment.
- Business environment is an access network which consists of several APs connected by a core network. Each AP serves a number of mobile terminals. HIPERLAN-2 also allows roaming between the APs.
- In home environment, an ad-hoc network is created.
- Fig. 4.4.5 presents the standard architecture of HIPERLAN-2 network.
- Two access points are connected to a **core network.**
- The Core network might be an ATM network, Ethernet LANs, UMTS 3G cellular network etc.
- Each access point contains two parts: an **Access Point Controller (APC)** and one or more **Access Point Transceiver (APT).**
- Four **mobile terminals (MT)** are also shown in Fig. 4.4.5.

These MTs can move from one cell area to another. The access point automatically selects a frequency by using (dynamic frequency selection) DFS.

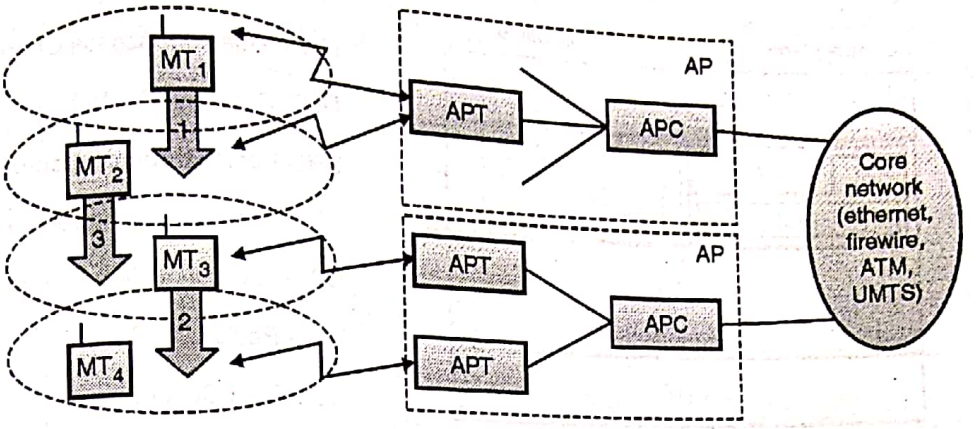


Fig. 4.4.5 : HIPERLAN/2 Basic structure and Handoff scenario

There are three types of handover which might occur :

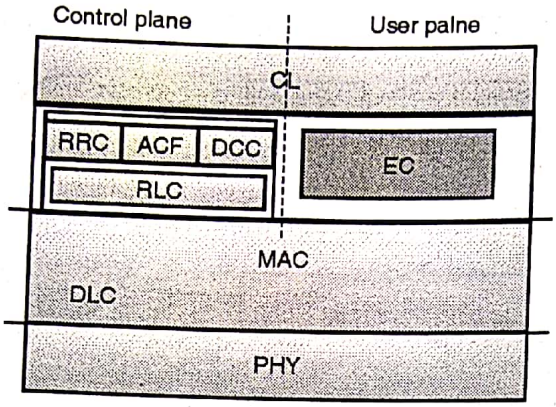
1. **Sector Handover (Inter sector)**
   - If the sectorized antennas are used for access point then AP supports this handover. MT moves from one sector to another sector that is controlled by the same APT.
   - Sector handover is handled inside the DLC layer therefore not visible outside the AP.
2. **Radio Handover (Inter-APT/Intra-AP)**
   - Radio handover is also handled within the AP.
   - As shown in Fig. 4.4.5, MT_3 moves from one APT to another APT of the same AP.
3. **Network Handover (Inter-AP/ Intra network)**
   - This handover occur when MT moves from one AP to another AP (in Fig. 4.4.6 MT_2).
   - In this case, the core network and higher layers are also involved.

HIPERLAN-2 networks operate in two modes

1. Centralized Mode (CM)
2. Direct Mode (DM)

1. **Centralized Mode (CM)**
   - This is an infrastructure based and mandatory mode.
   - All APs are connected to a core network and MTs are associated with APs.
   - If two MTs share the same cell then all data is transferred by AP.
   - AP takes complete control of everything.
2. **Direct Mode (DM)**
   - This is an ad-hoc and optional mode.
   - In this mode, data is directly exchanged between MTs if they can receive each other. But the network is still controlled by AP that contains a central controller (CC). The central controller can be connected to a core network and can operate in both centralized and direct modes.

HIPERLAN-2 Protocol Stack



MAC – Medium Access Control

DLC- Data Link Control

RRC-Radio Resource Control

ACF- Association Control Function

DCC-DLC connection control

RLC- Radio Link Control

EC – Error Control

CL – Convergence Layer

Fig. 4.4.6 : HIPERLAN-2 reference Model

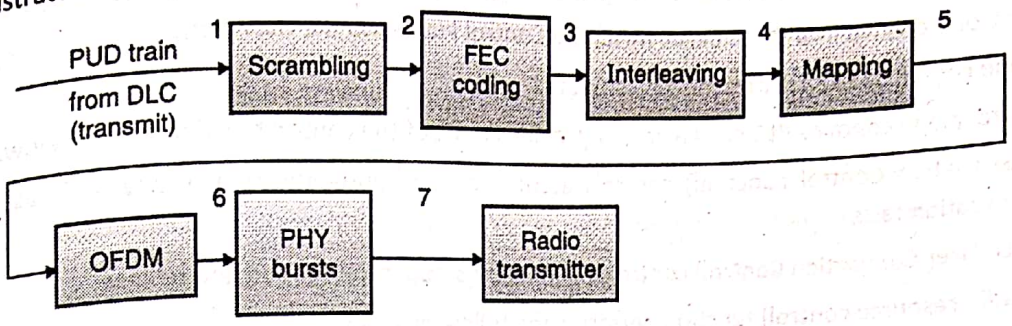
4.4.2(a) HIPERLAN-2 Physical Layer

- Many functions and features of PHY layer of HIPERLAN-2 are identical to IEEE 802.11a. It uses the same modulation scheme and provides the same data rate as IEEE 802.11a.
- Physical layer of HIPERLAN-2 performs the following functions.
  - Modulation(OFDM)
  - Forward Error Correction
  - Signal Detection
  - Synchronization etc.

Key features

- HIPERLAN-2 operates at **5GHz** frequency
- Maximum data rate of up to **54Mbit/s**
- It uses different modulation schemes such as BPSK, QPSK, 16-QAM, 64 –QAM to achieve different data rates.
- It employs **OFDM**.
- OFDM symbol duration - 4 µs
- Number of sub carriers - 52
- Number of pilot symbols - 4
- Subcarrier spacing - 312.5KHz
- Channel spacing - 20MHz
- Maximum transmit power is 200mW EIRP for the lower frequency band.

Fig. 4.4.7 illustrates the reference configuration of the transmission chain of a HIPERLAN-2 device.



1. Information bits
2. Scrambled bits
3. Encoded bits
4. Interleaved bits
5. Sub-carrier symbols
6. Complex baseband OFDM symbols
7. PHY bursts

Fig. 4.4.7 : HIPERLAN-2 Physical Layer reference configuration

The HIPERLAN-2 physical layer receives the PSDU from DLC Layer.

Step 1 : Scrambling

The first step then is scrambling of all data bits with the generator polynomial x^7+x^4+1. This is done for DC blocking and whitening of the spectrum. The outcome of this step is the scrambled bits.

Step 2 : FEC Coding

The next step is to apply FEC coding on these scrambled bits. This is done for error detection and correction. The result of this step is encoded bits.

Step 3 : Interleaving

Next, encoded bits are interleaved to mitigate the frequency selective fading. The result is interleaved bits.

Step 4 : Mapping

The mapping process first divides the bit sequence in group of 1, 2, 4 or 6 bits depending on the modulation schemes used such as BPSK, QPSK, 16-QAM,64-QAM respectively. These groups are mapped on to the appropriate modulation symbol. The result of this step is sub carrier modulation symbols.

Step 5 : OFDM Modulation

The OFDM modulation converts these symbols into a baseband signal. The symbol interval is 4μs.

Step 6 : PHY burst

In this step the physical burst is created. This burst contains preamble and payload.

Step 7 : Radio transmission

Finally radio transmission shifts the baseband signal into a carrier frequency.

4.4.2(b) HIPERLAN-2 Data Link Control Layer

- The Data Link control (DLC) layer is situated on top of the physical layer.
- DLC Layer contains the following sub functions :

1. MAC function
2. Error Control (EC)
3. RLC sub layer that in turn is sub divided into RLC, RRC, ACF and DCC.

- DLC layer provides for a logical link between MT and AP over the OFDM physical layer.
- Data link control is divided into three parts: MAC, the Control Plane and the User plane.
- The user plane contains Error Control mechanism (EC).
- And the control plane contains RLC sub layer that provides most of the control functions given below.
  - (i) ACF (Association Control Function) controls association and authentication of new MTs as well as performs synchronization task.
  - (ii) DCC (DLC User Connection Control) controls connection setup, modification and release.
  - (iii) RRC **(Radio resource control)** function performs the following tasks
    - Dynamic frequency selection
    - Measurements performed by MT
    - Reporting measurements to the AP
    - Frequency change by the AP and its associated MTs
    - Power saving procedure
    - Transmit power control
    - Handover between APs and within AP
- Fig. 4.4.8 shows HIPERLAN-2 MAC Frame format.

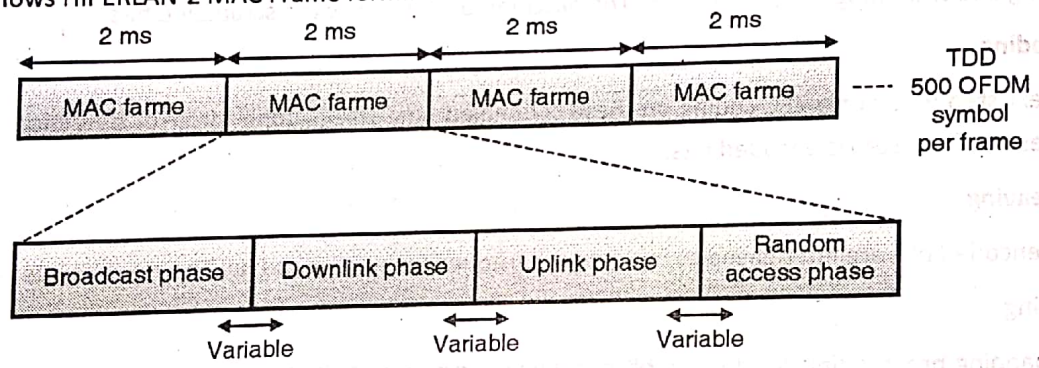


Fig. 4.4.8 : MAC frame structure of HIPERLAN-2

- HIPERLAN-2 medium access control is based on the TDMA/TDD.
- Each MAC frame is of 2ms duration and it is further divided into four phases.
  - **Broadcast Phase :** Carries the Broadcast Control Channel (BCCH) and Frame Control Channel (FCCH).
  - **Downlink phase :** Carries information from access point (AP) or Central Controller (CC) to the specified mobile terminal.
  - **Uplink phase :** Carries information from mobile terminal to AP or CC.
  - **Random access phase :** Used to transmit random access channel (RCH) .
- HIPERLAN-2 defines six different transport channels
  - **BCH (Broadcast channel) :** This channel conveys basic information for the radio cell to all MTs.
  - **FCH (Frame channel) :** Contains the exact description of the allocation of resources within the current MAC frame.

- **ACH (Access feedback channel) :** Gives feedback to MTs regarding random access during the RCH of the previous frame.
- **LCH (Long support channel) :** Transports user and control data for downlinks and uplinks.
- SCH (Short transport channel) : Transports control data for downlinks and uplinks.
- **RCH (Random channel) :** Using this channel, MTs can send information to AP/CC via slotted Aloha.

- HIPERLAN-2 also defines some logical channels for signaling, control and information transfer. These logical channels are mapped on SCH, LCH, and RCH transport channels.
  - **SBCH :** Used only in downlink to broadcast control information related to the cell. It helps in handover, association, security and radio link control functions.
  - **DCCH :** Conveys RLC sub layer signals between an AP and the MT.
  - **UDCH :** Carries DLC PDU for convergence layer data.
  - **LCCH :** It is used for error control functions for a specific UDCH.
  - **ASCH :** It is used for association and re-association request messages.

4.5 Bluetooth

4.5.1 Introduction

- Bluetooth is a wireless LAN technology with very limited coverage (about 10m) and it does not need any infrastructure (Bluetooth is an example of ad hoc networks).
- Bluetooth technology was first developed by Ericsson. It was then formalized by a group of electronics manufacturers such as Ericsson, IBM, Intel, Nokia, and Toshiba who jointly form the Bluetooth Special Interest Group (SIG).
- Bluetooth technology was designed primarily to support simple wireless networking of personal consumer devices and peripherals, including cell phones, PDAs, and wireless headsets (Personal Area Network – PAN).
- Compared to Wi-Fi, Bluetooth networking is much slower, a bit more limited in range, and supports fewer devices.

Features of Bluetooth

- Bluetooth devices generally communicate at less than 1 Mbps.
- Operates in the **2.4 GHz** ISM band with 79 or 23 RF channels.
- GFSK (Gaussian Frequency Shift Keying) modulation is used and TDD (Time Division Duplex) is used for uplink and downlink separation.
- It applies **FHSS** with a **1600** hops/s hopping rate.
- It uses SCO (Synchronous Connection Oriented) links for voice and ACL (Asynchronous Connection less) links for Data.
- Uses FEC (forward error correction) with no retransmission.
- Uses 64 kbit/s duplex, point-to-point, circuit switched channels.
- Topology : Overlapping piconets (stars) forming a scatternet.

4.5.2 User Scenario

Many different configurations with Bluetooth based piconet are possible.

1. **Connection of peripheral devices :** Today most of the devices use wires to connect to the peripheral devices such as keyboard, mouse, headset, speakers etc. Each type of device has its own type of cable, connectors, plugs etc. In a wireless networks no wires are needed to connect such devices. Bluetooth piconet can be used to connect such peripherals without wires to the wireless terminals such as laptop or PDA.
2. **Support for ad hoc networking :** Ad-hoc networks are useful for tradeshows and exhibitions where several people come together and exchange data. Wireless networks can support this type of interaction. Small devices may not have WLAN adapters of IEEE802.11 standard, but cheaper Bluetooth chips built in.
3. **Bridging of Networks :** Using wireless piconets, a mobile phone can be connected to a PDA or laptop in a simple way. The mobile phone that has bluetooth chip can now act as a bridge between the local piconet and the global GSM network.

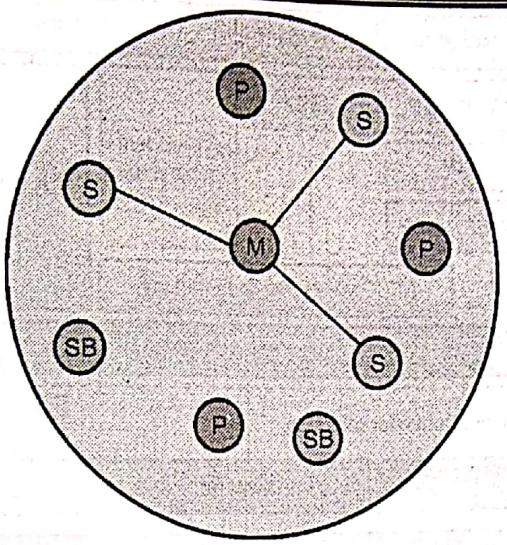
4.5.3 Architecture

MU – May 14

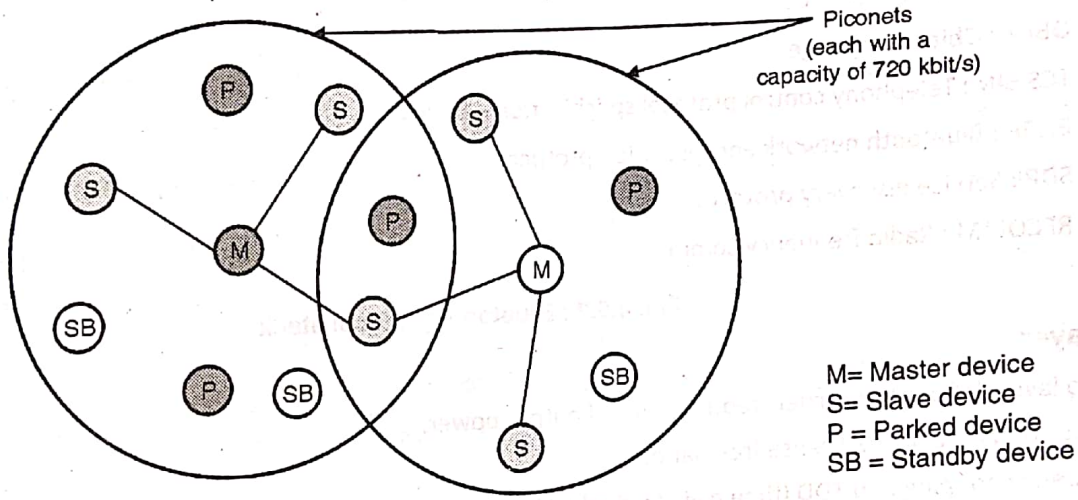
Q. With respect to Bluetooth protocol explain piconet and scatternet. **(May 14, 10 Marks)**

Piconet and Scatternet

1. **Piconet**
   - **Piconet** is a collection of Bluetooth devices which are synchronized to the same hopping sequence.
   - Each piconet has one device called Master (M). All other devices called slaves (S) are connected to the master.
   - The master determines the hopping sequence in the piconet and all slaves have to synchronize to this pattern. If a device wants to participate it has to synchronize to this.
   - There are two more types of devices: Parked device (P) and Stand-by devices(SB).
     - Parked devices can not actively participate in the piconet but are known and can be reactivated within some milliseconds.
     - Stand-by (SB) devices do not participate in the piconet.
   - A Master (M) can connect seven active slaves and up to 255 parked slaves per piconet.
   - All active devices in a piconet are assigned a 3-bit active member address (AMA). And all parked devices are assigned 8-bit parked member address (PMA).
   - The master (M) gives its clock and 48-bit device ID to all slaves in a piconet. Hopping sequence is determined by device ID and hopping pattern is determined by master's clock.
   - All active devices use the same hopping sequence and hops together.



(a)



(b)

Fig. 4.5.1 : (a) Piconet (b) Scatternet

2. **Scatternet**

- **Scatternet** is a group of piconets. More than one piconet can be connected to form a scatternet through the sharing of common master or slave devices.
- Devices can be slave in one piconet and master in another.
- Communication between piconets can take place by jumping devices back and forth between the piconets.
- Each piconet in a scatternet uses a different hopping sequence that is always determined by the master of that piconet.

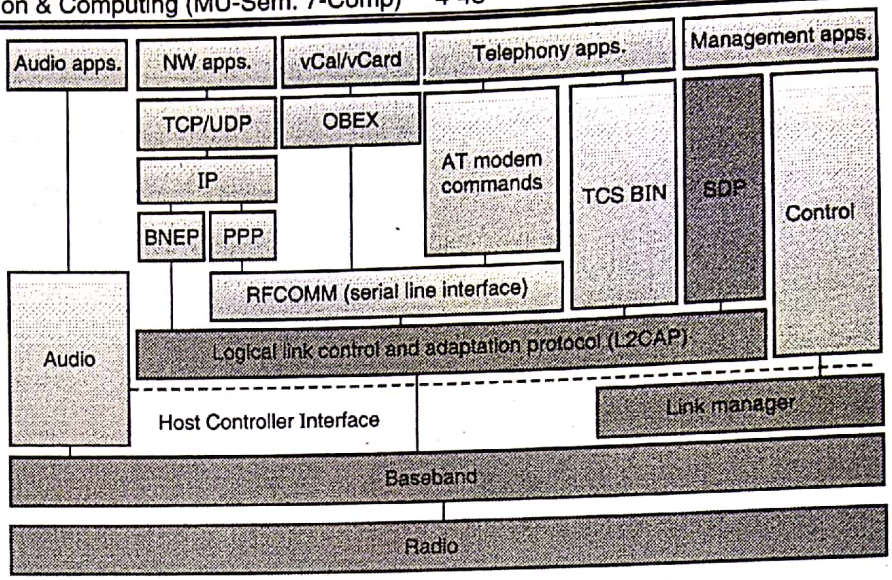
4.5.4 Bluetooth Protocol Stack

MU – May 12, Dec. 12, Dec. 13, May 16, Dec. 16, May 17, Dec. 17, May 18, Dec. 18

Q. Draw and explain Bluetooth protocol stack in detail. **(May 12, Dec. 12, Dec. 13, Dec. 18, 10 Marks)**

Q. Explain in detail Bluetooth protocol architecture. **(May 16, Dec. 16, May 17, May 18, 10 Marks)**

Q. Describe Bluetooth architecture and protocol stack. Also discuss its limitations. **(Dec. 17, 10 Marks)**



- AT : Attention sequence
- OBEX : Object exchange
- TCS BIN : Telephony control protocol specification – binary
- BNEP : Bluetooth network encapsulation protocol
- SDP : Service discovery protocol
- RFCOMM : Radio frequency comm.

Fig. 4.5.2 : Bluetooth protocol stack

Radio Layer

- Radio layer defines the carrier frequencies and output power.
- Bluetooth uses 2.4 GHZ license free band.
- Frequency hopping and TDD (time division duplex) is used for transmission with fast hopping rate of 1600 hops/s.
- It uses 79 hop carriers equally spaced with 1 MHz.
- Gaussian FSK used for modulation.

Baseband Layer

- Baseband layer performs frequency hopping to avoid interference and to access the medium.
- Defines physical links and many packet formats.
- It controls :
  - Device Addressing
  - Channel control (how devices find each other) through paging and inquiry methods
  - Power-saving operations
  - Flow control and synchronization among Bluetooth devices.

Link Manager Protocol (LMP)

- The link manager protocol (LMP) manages various aspects of the radio link between master and slave.
- The following functions are covered by LMP :
  - Authentication, pairing, and encryption
  - Synchronization
  - Capability negotiation

- QoS negotiation
- Power control
- Link supervision
- State and transmission mode change

Logical Link Control and Adaptation Layer Protocol (L2CAP)

- L2CAP is layered over the Baseband Protocol and resides in the data link layer.
- L2CAP provides :
  - Connection-oriented and connectionless data services to upper layer protocols with protocol multiplexing capability.
  - Segmentation and reassembly operation.
  - Group abstractions.
- L2CAP provides three different types of logical channels that are transported via ACL link between master and slave, these are :
  - Connectionless used for broadcast.
  - Connection-oriented for data transfer with QoS flow specification.
  - Signaling used to exchange signaling messages between L2CAP entities.

Host Controller Interface (HCI)

- The HCI provides a command interface to the baseband controller and link manager
- It provides access to hardware status and control registers.
- Essentially this interface provides a uniform method of accessing the Bluetooth baseband capabilities.
- The HCI exists across 3 sections, **The Host, Transport Layer, Host Controller**. Each of the sections has a different role to play in the HCI system.
- HCI defines the set of functions of a Bluetooth module that are accessible to the host and its application.
- HCI can be seen as a software/hardware boundary.

RFCOMM

- The RFCOMM protocol provides emulation of serial ports over the L2CAP protocol.
- It is a cable replacement protocol that provides a serial line interface to all the applications.
- The protocol is based on the ETSI standard TS 07.10.
- It supports multiple serial ports over a single physical channel.

Service Discovery Protocol (SDP)

- The service discovery protocol (SDP) helps the applications to discover which services are available and to determine the characteristics of those available services.
- SDP defines only the discovery of services not about their usage.
- New service is discovered as follows
  - Client sends a request to search for an interested service.
  - Then server responds to the client with the list of available services that match to client's criteria.
  - The client uses this list to retrieve additional service attribute for the service of interest.

Profiles

- Profiles are specifications which describe how Bluetooth should be used in a specific application and as thus ensures that all devices from different manufacturers can seamlessly work with one another. There are about a dozen profiles:
- Generic Access, Serial Port, Dialup Networking, FAX, Headset, LAN Access Point, Generic Object Exchange (OBEX), File Transfer, Object Push, Synchronization, Cordless Telephony, and Intercom.
- More profiles are under discussion within various Bluetooth SIG groups.
- The profile concept is used to decrease the risk of interoperability problems between different manufacturers' products.

Telephony Control Protocol Specification Binary (TCS-BIN)

To define call control signaling for the establishment of voice and data calls between Bluetooth devices TCS-BIN describes a binary, packet based, bit-oriented protocol.

4.5.4(a) Bluetooth Baseband States

MU – Dec. 15

Q. Explain how a Bluetooth network is established using baseband state transitions. **(Dec. 15, 10 Marks)**

- A typical Bluetooth device has a power of 100mW and can have a range of upto 100m.
- Having such huge power and relying on battery as its source will result in a huge wastage if the device lies idle for long time.
- Bluetooth defines several low-power states for a device. The major states present can be seen in the Fig. 4.5.3.
- **Standby :** A device which is currently ON and not part of any piconet is in standby mode. In this low-power mode only the native-clock runs.
- **Inquiry :** Now the movement to the next node i.e. inquiry state is based on either of two ways :
  1. **A device wants to establish a piconet :** The user wants to scan all the devices in its range. This inquiry procedure is started by sending an Inquiry access Code (IAC) to all devices in range.
  2. **Device in Standby that listens periodically :** A device which is in Standby may enter the Inquiry state periodically to search for IAC messages. If it finds one such, then it transfers the necessary information about itself and becomes a slave.
- **Page mode :** On successful inquiry, the device enters the page mode. In the page state two different roles are defined.
  1. After the master finds all the devices required for a connection, it sets up a piconet.
  2. The master then calculates special hopping sequences based on the device addresses received to contact each device individually.
  3. The slaves answer to calls by the master and synchronize their clocks accordingly.
  4. In the meantime, the master may continue to page more devices to the piconet.
  5. As soon as the device (slave) synchronizes to the hopping pattern of the piconet, it enters the connected state.
- **Connected :** The connected state contains the active state and three low power states.
- **Active :**
  - In active state the slave participates in the piconet by listening, transmitting and receiving. A master periodically synchronizes with these slaves.
  - The communication is done via ACL and SCO links.
  - Every device which is active needs to have a 3-bit Active Member Address (AMA).
  - In the active state, if the device is not transmitting, it can disconnect itself and go to standby by **detach** method.

A Bluetooth also has the choice to go into either of the three low-power states which are :

1. **Sniff**
   - Out of all the three low power states, this one has max. power consumption.
   - Unlike in active state where the slave listens to piconet at every slot, here it listens at a reduced rate which can be programmed as per the need.
   - The master also allocates a reduced number of slots for the slave in sniff mode.
2. **Hold**
   - The device here stops all ACL link transmissions are stopped.
   - If no activity is there in the piconet, the slave reduce the power consumption or participates in another piconet.
3. **Park**
   - This state has the lower duty cycle and lowest power consumption of the three.
   - It also release it 3-bit AMA address. Instead it gets a 8-bit PMA (Parked Member Access).
   - It remains a member of the piconet but gives a chance for another device to become active.

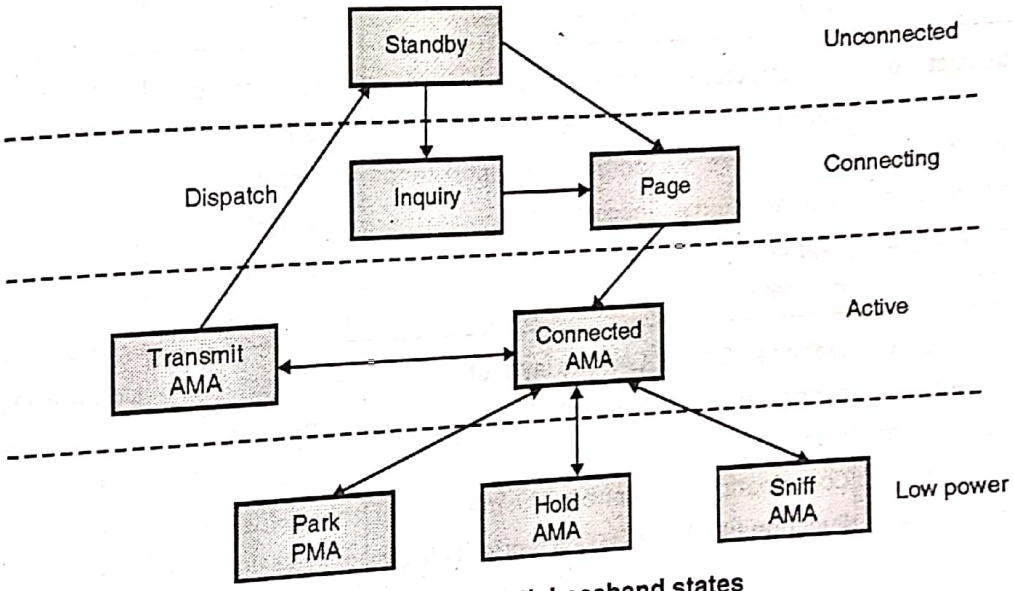


Fig. 4.5.3 : Bluetooth baseband states

4.6 Comparison of IEEE 802.11, HIPERLAN-1, HIPERLAN-2 and Bluetooth

MU - Dec. 12, Dec. 13, May 15, Dec. 15, May 16, Dec. 16, Dec. 17

Q. Compare between IEEE 802.11 and HIPERLAN-2. (Dec. 12, Dec. 13, Dec. 17, 10 Marks)

Q. Compare HIPERLAN-1, HIPERLAN-2 and 802.11 W-LAN. (May 15, 10 Marks)

Q. Write a short note on HIPER LAN-1 VS HIPERLAN-2. (Dec. 15, 5 Marks)

Q. Compare HIPERLAN 2, BLUETOOTH, IEEE 802.11. (May 16, Dec. 16, 10 Marks)

Table 4.6.1 : Comparison of IEEE 802.11, HIPERLAN and Bluetooth

Characteristic	IEEE 802.11	IEEE 802.11a	HIPERLAN-1	HIPERLAN-2	Bluetooth
Frequency	2.4 GHz	5GHz	5 GHz	5GHz	2.4 GHz
Max data rate	2 Mbps (11 Mbps with CCK)	54 Mbps	23.5Mbps	54 Mbps	<1Mbps

Characteristic	IEEE 802.11	IEEE 802.11a	HIPERLAN-1	HIPERLAN-2	Bluetooth
User throughput	6 Mbps	34Mbps	<20Mbps	34Mbps	<1Mbps
Connection	Point-to-point	Point-to-Multipoint	Provide multi-hop routing	Point-to-Multipoint	Point-to-Multipoint
Physical layer	FHSS/DSSS	OFDM	–	OFDM	FHSS
Authentication	None	None	None	x.509	Yes
Medium access	CSMA/CA	CSMA/CA	Variant of CSMA/CA i.e. EYNPMA protocol	CSMA/CA	Master is responsible for Medium access.
Transmit power	100mW	0.05/0.25/1W TPC	0.01/0.1/1 W	0.2 to 1 W	1 to 100 mW
Error control	ARQ	ARQ,FEC at PHY layer	FEC at Physical layer. It uses BCH codes.	ARQ/FEC at PHY layer	ARQ/FEC at MAC layer
Architecture	Infrastructure based architecture with additional support for ad hoc networks	Infrastructure based architecture with additional support for ad hoc networks	Infrastructure based architecture with additional support for ad hoc networks	Infrastructure based architecture with additional support for ad hoc networks	Ad hoc network
QoS support	Optional -QoS is supported by providing Point Coordination Function (PCF)	Optional -QoS is supported by providing Point Coordination Function (PCF)	CAC sub layer of HIPERLAN1 provides five priority levels for QoS support. The mapping of a QoS on a priority level is done with the help of packet life time	Yes: Uses connection oriented service to provide QoS such as bandwidth, delay, jitter etc.	Link Manager protocol provides means to negotiate QoS such as flow specification.
Connectivity	Connectionless	Connectionless	Connection less	Connection-oriented	Connectionless+connection-oriented

Review Questions

Q. 1 Discuss the advantages and disadvantages of WLAN over wired network. Explain two basic types of WLAN architecture.

Q. 2 Explain in detail function of HIPERLAN-1 CAC sublayer.

Q. 3 Draw and explain IEEE 802.11 protocol architecture.

Q. 4 Discuss the PHY frame format of an IEEE 802.11 using FHSS technique.

Q. 5 Describe IEEE 802.11 MAC frame format.

Q. 6 Describe MAC mechanism schemes used in IEEE802.11. Explain in detail MAC scheme that uses DCF with RTS/CTS extension.

Q. 7 Discuss Basic MAC schemes used in IEEE 802.11.

Q. 8 Write a short note on HIPERLAN-2.

Q. 9 Explain HIPERLAN-2 data link control layer.

□□□