BACHELOR OF COMPUTER APPLICATIONS

SEMESTER 3

DCA2104

BASICS OF DATA COMMUNICATION

Unit 14

Wireless LANs

Table of Contents

1. INTRODUCTION

This unit introduces the concept of Wireless LANs. Wireless communication is one of the fastest-growing technologies. The demand for connecting devices without the use of cables is increasing everywhere. Wireless LANs can be found on college campuses, in office buildings and in many public areas.

In this unit, we are going to discuss IEEE 802.11 architecture. In the next section we will discuss IEEE802.11 medium access control sublayer. Then we will discuss addressing mechanisms in IEEE802.11. In this unit, we will also discuss IEEE802.11 physical layer. In the last section, we will discuss Bluetooth's 7 – layer architecture.

1.1 Objectives

After studying this unit, you should be able to:

- *Describe IEEE802.11 architecture*
- *Explain IEEE802.11 addressing mechanism*
- *Describe IEEE802.11 physical layer and MAC sublayer*
- *Explain bluetooth architecture*
- *Describe bluetooth layers*

2. IEEE802.11

IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data link layers.

2.1 Architecture

In 1990, the IEEE 802 Committee formed a new working group, IEEE 802.11, specifically devoted to wireless LANs, with a charter to develop a MAC protocol and physical medium specification. But keeping pace with the demand, the IEEE 802.11 working group has issued an ever-expanding list of standards as given in the table 14.1. Table 14.2 briefly defines key terms used in the IEEE 802.11 standard.

The first 802.11 standard to gain broad industry acceptance was 802.11b. The Wireless Ethernet Compatibility Alliance (WECA), an industry consortium formed in 1999 later renamed as the Wi-Fi (Wireless Fidelity) Alliance, created a test suite to certify interoperability for 802.11b products. The term used for certified 802.11b products is Wi-Fi. Wi-Fi certification has been extended to 802.11g products. The Wi-Fi Alliance has also developed a certification process for 802.11a products, called Wi-Fi5. The Wi-Fi Alliance is concerned with a range of market areas for WLANs, including enterprise, home, and hot spots.

Table 14.1: IEEE 802.11 Standards

Standard	Scope
IEEE 802.11	Medium access control (MAC): One common MAC for WLAN applications
	Physical layer: Infrared at 1 and 2 Mbps
	Physical layer: 2.4-GHz FHSS at 1 and 2 Mbps
	Physical layer: 2.4-GHz DSSS at 1 and 2 Mbps
IEEE 802.11a	Physical layer: 5-GHz OFDM at rates from 6 to 54 Mbps
IEEE 802.11b	Physical layer: 2.4-GHz DSSS at 5.5 and 11 Mbps
IEEE 802.11c	Bridge operation at 802.11 MAC layer
IEEE 802.11d	Physical layer: Extend operation of 802.11 WLANs to new regulatory domains (countries)
IEEE 802.11e	MAC: Enhance to improve quality of service and enhance security mechanisms
IEEE 802.11f	Recommended practices for multivendor access point interoperability
IEEE 802.11g	Physical layer: Extend 802.11b to data rates >20 Mbps
IEEE 802.11h	Physical/MAC: Enhance IEEE 802.11a to add indoor and outdoor channel selection and to improve spectrum and transmit power management
IEEE 802.11i	MAC: Enhance security and authentication mechanisms
IEEE 802.11j	Physical: Enhance IEEE 802.11a to conform to Japanese requirements
IEEE 802.11k	Radio resource measurement enhancements to provide interface to higher layers for radio and network measurements
IEEE 802.11m	Maintenance of IEEE 802.11-1999 standard with technical and editorial corrections
IEEE 802.11n	Physical/MAC: Enhancements to enable higher throughput
IEEE 802.11p	Physical/MAC: Wireless access in vehicular environments
IEEE 802.11r	Physical/MAC: Fast roaming (fast BSS transition)
IEEE 802.11s	Physical/MAC: ESS mesh networking
IEEE 802.11,2	Recommended practice for the evaluation of 802.11 wireless performance
IEEE 802.11u	Physical/MAC: Interworking with external networks

Table 14.2: IEEE 802.11 Terminology

Access point (AP)	Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations
Basic service set (BSS)	A set of stations controlled by a single coordination function
Coordination function	The logical function that determines when a station operating within a BSS is permitted to transmit and may be able to receive PDUs
Distribution system DS	A system used to interconnect a set of BSSs and integrated LANs to create an (ESS)
Extended service set (ESS)	A set of one or more interconnected BSSs and integrated LANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs
MAC protocol data unit (MPDU)	The unit of data exchanged between two peer MAC entites using the services of the physical layer
MAC service data unit (MSDU)	Information that is delivered as a unit between MAC users
Station	Any device that contains an IEEE 802.11 conformant MAC and physical layer

IEEE 802.11 Architecture

Figure 14.1 shows the IEEE 802.11 architecture.

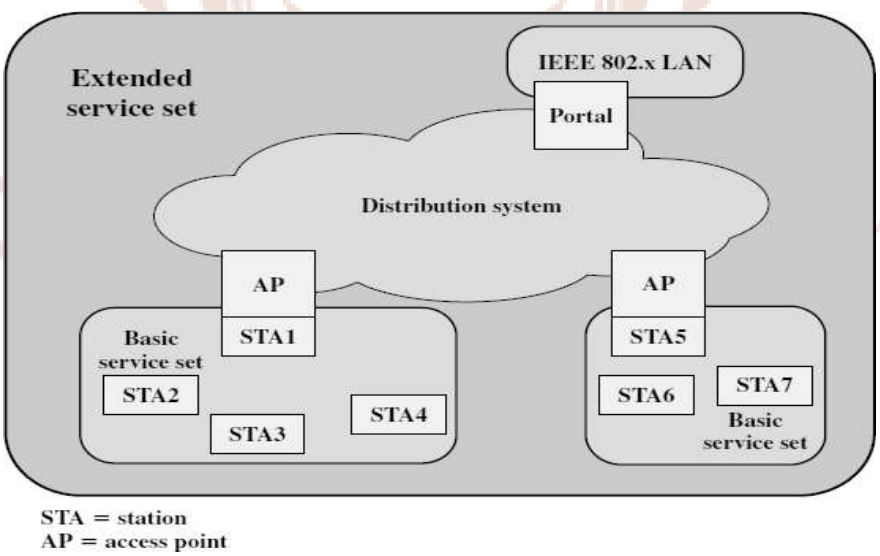

Fig 14.1: IEEE 802.11 Architecture

Basic service set (BSS), is the smallest building block of a wireless LAN. It consists of some number of stations executing the same MAC protocol and competing for access to the same shared wireless medium. You can isolate or connect a BSS to a backbone **distribution**

system (DS) through an **access point (AP).** The AP functions as a bridge and a relay point. In a BSS, client stations do not communicate directly with one another. Rather, if one station in the BSS wants to communicate with another station in the same BSS, the MAC frame is first sent from the originating station to the AP, and then from the AP to the destination station. Similarly, a MAC frame from a station in the BSS to a remote station is sent from the local station to the AP and then relayed by the AP over the DS on its way to the destination station. The BSS generally is referred to as a cell. The DS can be a switch, a wired network, or a wireless network.

When all the stations in the BSS are mobile stations, with no connection to other BSSs, the BSS is called an **independent BSS (IBSS).** An IBSS is typically an ad hoc network. In IBSS, the stations all communicate directly, and no AP is involved. A simple configuration is shown in figure 14.1, in which each station belongs to a single BSS; that is, each station is within wireless range only of other stations within the same BSS. It is also possible for two BSSs to overlap geographically, so that a single station could participate in more than one BSS. Further, the association between a station and a BSS is dynamic. Stations may turn off, come within range, and go out of range.

An **extended service set (ESS)** consists of two or more basic service sets interconnected by a distribution system. Typically, the distribution system is a wired backbone LAN but can be any communications network. The extended service set appears as a single logical LAN to the logical link control (LLC) level. Figure 14.1 indicates that an access point (AP) is implemented as part of a station; the AP is the logic within a station that provides access to the DS by providing DS services in addition to acting as a station. To integrate the IEEE 802.11 architecture with a traditional wired LAN, a portal is used. The portal logic is implemented in a device, such as a bridge or router, that is part of the wired LAN and that is attached to the DS.

IEEE 802.11 Services

Let's look at the services defined for IEEE 802.11 standard. Table 14.3 lists the services defined by IEEE 802.11 that need to be provided by the wireless LAN to provide functionality.

Table 14.3: IEEE 802.11 Services

Service	Provider	Used to Support
Association	Distribution system	MSDU delivery
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Dissassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery
Privacy	Station	LAN access and security
Reassocation	Distribution system	MSDU delivery

The service provider can be either the station or the DS. Station services are implemented in every 802.11 station, including AP stations. Distribution services are provided between BSSs. Three of the services are used to control IEEE 802.11 LAN access and confidentiality. Six of the services are used to support delivery of MAC service data units (MSDUs) between stations. The MSDU is a block of data passed down from the MAC user to the MAC layer.

The two services involved with the distribution of messages within a DS are **distribution** and **integration**. **Distribution** is the primary service used by stations to exchange MAC frames when the frame must traverse the DS to get from a station in one BSS to a station in another BSS.

The **integration** service enables transfer of data between a station on an IEEE 802.11 LAN and a station on an integrated IEEE 802.x LAN. The integration service takes care of any address translation and media conversion logic required for the exchange of data.

Association-Related Services The primary purpose of the MAC layer is to transfer MSDUs between MAC entities; this purpose is fulfilled by the distribution service. For that service to function, it requires information about stations within the ESS that is provided by the association-related services. Before the distribution service can deliver data to or accept data from a station, that station must be associated. Before looking at the concept of association, we need to describe the concept of mobility. The standard defines three transition types, based on mobility:

- **No transition:** A station of this type is either stationary or moves only within the direct communication range of the communicating stations of a single BSS.
- **BSS transition:** This is defined as a station movement from one BSS to another BSS within the same ESS. In this case, delivery of data to the station requires that the addressing capability be able to recognize the new location of the station.
- **ESS transition:** This is defined as a station movement from a BSS in one ESS to a BSS within another ESS.

To deliver a message within a DS, the distribution service needs to know where the destination station is located. Specifically, the DS needs to know the identity of the AP to which the message should be delivered in order for that message to reach the destination station. To meet this requirement, a station must maintain an association with the AP within its current BSS. Three services relate to this requirement:

- **Association:** Establishes an initial association between a station and an AP.
- **Reassociation:** Enables an established association to be transferred from one AP to another, allowing a mobile station to move from one BSS to another.
- **Disassociation:** A notification from either a station or an AP that an existing association is terminated. A station should give this notification before leaving an ESS or shutting down.

2.2 Medium Access Control Sublayer

The IEEE 802.11 MAC layer covers three functional areas: reliable data delivery, access control, and security. Let see the first two topics in this section.

Reliable Data Delivery

A wireless LAN using the IEEE 802.11 physical and MAC layers is subject to considerable unreliability. Noise, interference, and other propagation effects result in the loss of a significant number of frames. So deal errors at the MAC level more efficiently, IEEE 802.11 includes a frame exchange protocol. When a station receives a data frame from another station, it returns an acknowledgment (ACK) frame to the source station. If the source does not receive an ACK within a short period, either because its data frame was damaged or because the returning ACK was damaged, the source retransmits the frame. Thus, the basic data transfer mechanism in IEEE

802.11 involves an exchange of two frames. To further enhance reliability, a four-frame exchange may be used. In this scheme, a source first issues a Request to Send (RTS) frame to the destination. The destination then responds with a Clear to Send (CTS). After receiving the CTS, the source transmits the data frame, and the destination responds with an ACK. The RTS alerts all stations that are within reception range of the source that an exchange is under way; these stations refrain from transmission in order to avoid a collision between two frames transmitted at the same time. Similarly, the CTS alerts all stations that are within reception range of the destination that an exchange is under way. The RTS/CTS portion of the exchange is a required function of the MAC but may be disabled.

Medium Access Control

The 802.11 working group considered two types of proposals for a MAC algorithm: distributed access protocols, which distribute the decision to transmit over all the nodes using a carrier sense mechanism; and centralized access protocols, which involve regulation of transmission by a centralized decision maker. A distributed access protocol makes sense for an ad hoc network of peer workstations (typically an IBSS) and may also be attractive in other wireless LAN configurations that consist primarily of bursty traffic. A centralized access protocol is natural for configurations in which a number of wireless stations are interconnected with each other and some sort of base station that attaches to a backbone wired LAN. The end result for 802.11 is a MAC algorithm called DFWMAC (distributed foundation wireless MAC) that provides a distributed access control mechanism with an optional centralized control built on top of that. Figure

14.2 illustrates the IEEE 802.11 Protocol Architecture.

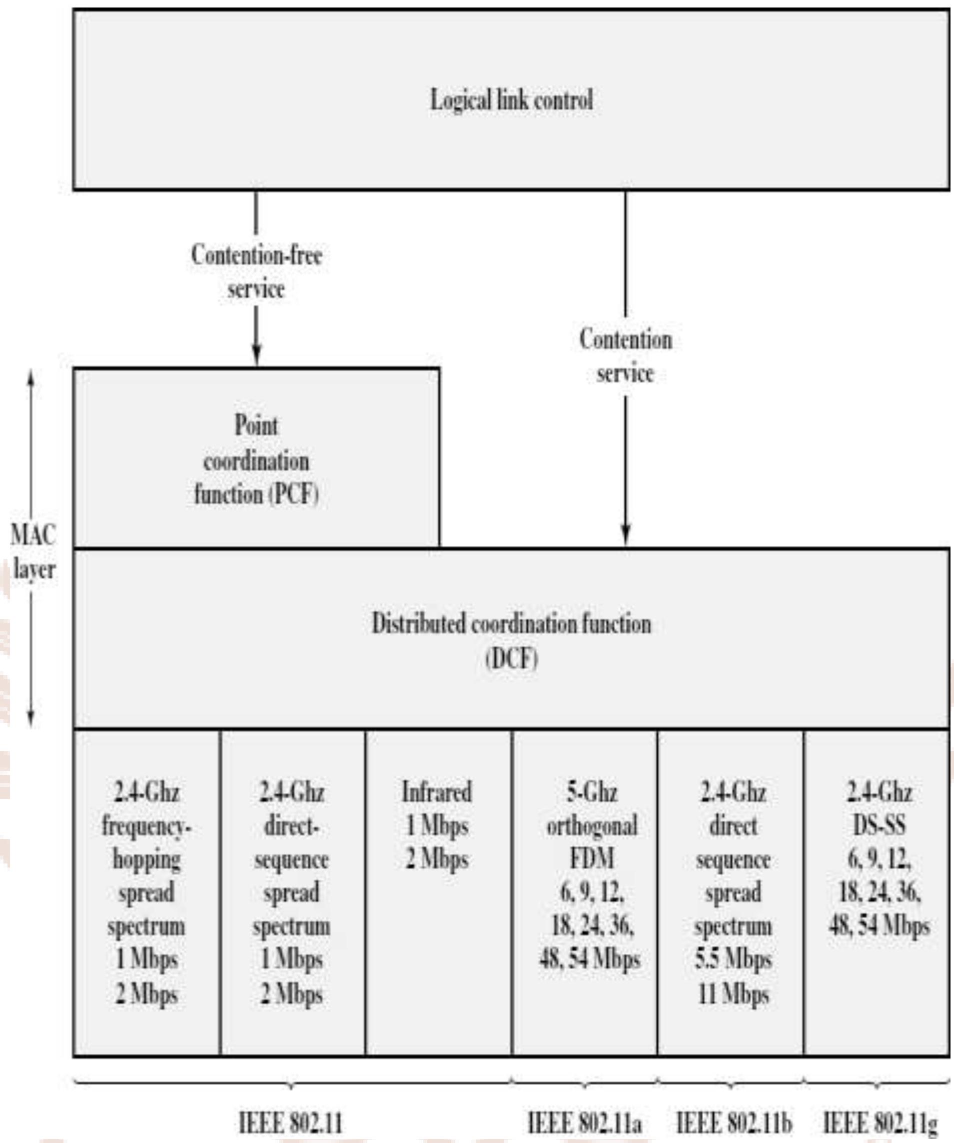

Fig 14.2: IEEE 802.11 Protocol Architecture

The lower sublayer of the MAC layer is the distributed coordination function (DCF) which uses a contention algorithm to provide access to all traffic.

Ordinary asynchronous traffic directly uses DCF. The point coordination function (PCF) is a centralized MAC algorithm used to provide contention- free service. PCF is built on top of DCF and exploits features of DCF to assure access for its users. Let us discuss these two sublayers.

Distributed Coordination Function: The DCF sublayer makes use of a simple CSMA (carrier sense multiple access) algorithm. If a station has a MAC frame to transmit, it listens to the medium. If the medium is idle, the station may transmit; otherwise the station must wait until the current transmission is complete before transmitting.

DCF includes a set of delays that amounts to a priority scheme. Let us start by considering a single delay known as an interframe space (IFS). Using an IFS, the rules for CSMA access are as follows (Figure 14.3):

1. A station with a frame to transmit senses the medium. If the medium is idle, it waits to see if the medium remains idle for a time equal to IFS. If so, the station may transmit immediately.
2. If the medium is busy the station defers transmission and continues to monitor the medium until the current transmission is over.
3. Once the current transmission is over, the station delays another IFS. If the medium remains idle for this period, then the station backs off a random amount of time and again senses the medium. If the medium is still idle, the station may transmit. During the backoff time, if the medium becomes busy, the backoff timer is halted and resumes when the medium becomes idle.
4. If the transmission is unsuccessful, which is determined by the absence of an acknowledgement, then it is assumed that a collision has occurred.

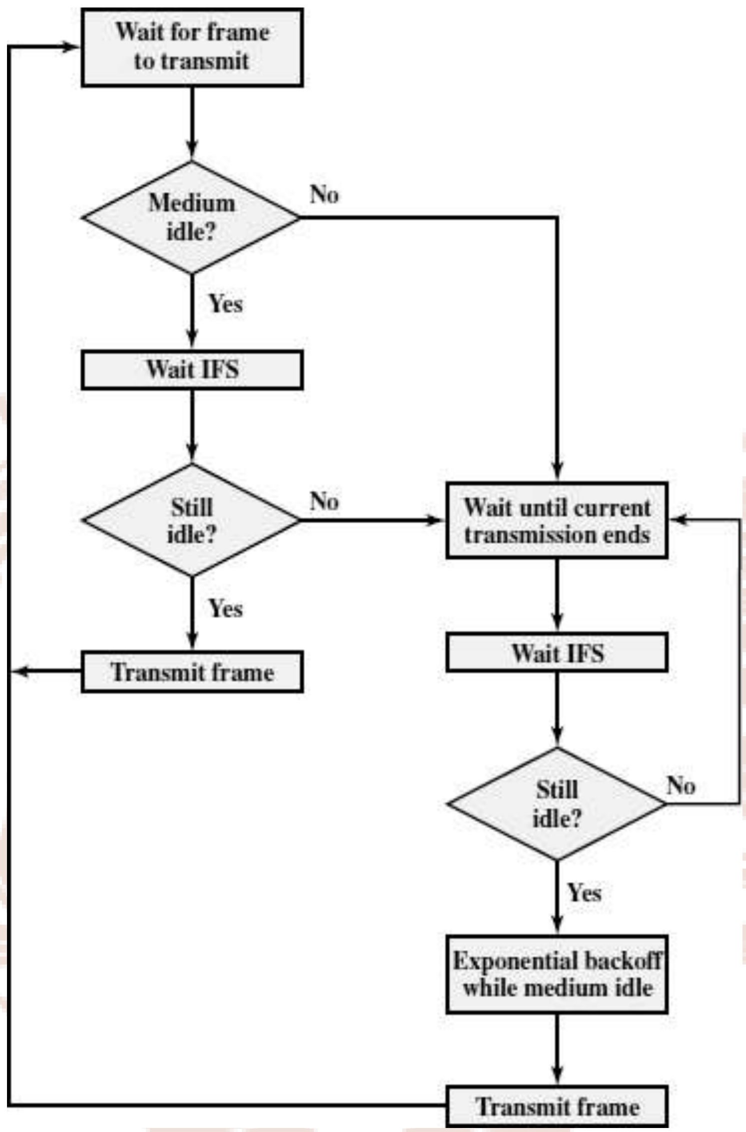

Fig 14.3: IEEE 802.11 Medium Access Control Logic

Here binary exponential backoff is used in order to ensure that backoff maintains stability. Binary exponential backoff provides a means of handling a heavy load. Repeated failed attempts to transmit result in longer and longer backoff times, which helps to smooth out the load. Without such a backoff, the following situation could occur: Two or more stations attempt to transmit at the same time, causing a collision. These stations then immediately attempt to retransmit, causing a new collision. The preceding scheme is refined for DCF to provide priority-based access by the simple expedient of using three values for IFS:

- **SIFS (short IFS):** The shortest IFS, used for all immediate response actions

- **PIFS (point coordination function IFS):** A midlength IFS, used by the centralized controller in the PCF scheme when issuing polls
- **DIFS (distributed coordination function IFS):** The longest IFS, used as a minimum delay for asynchronous frames contending for access

Figure 14.4 (a) illustrates the use of these time values.

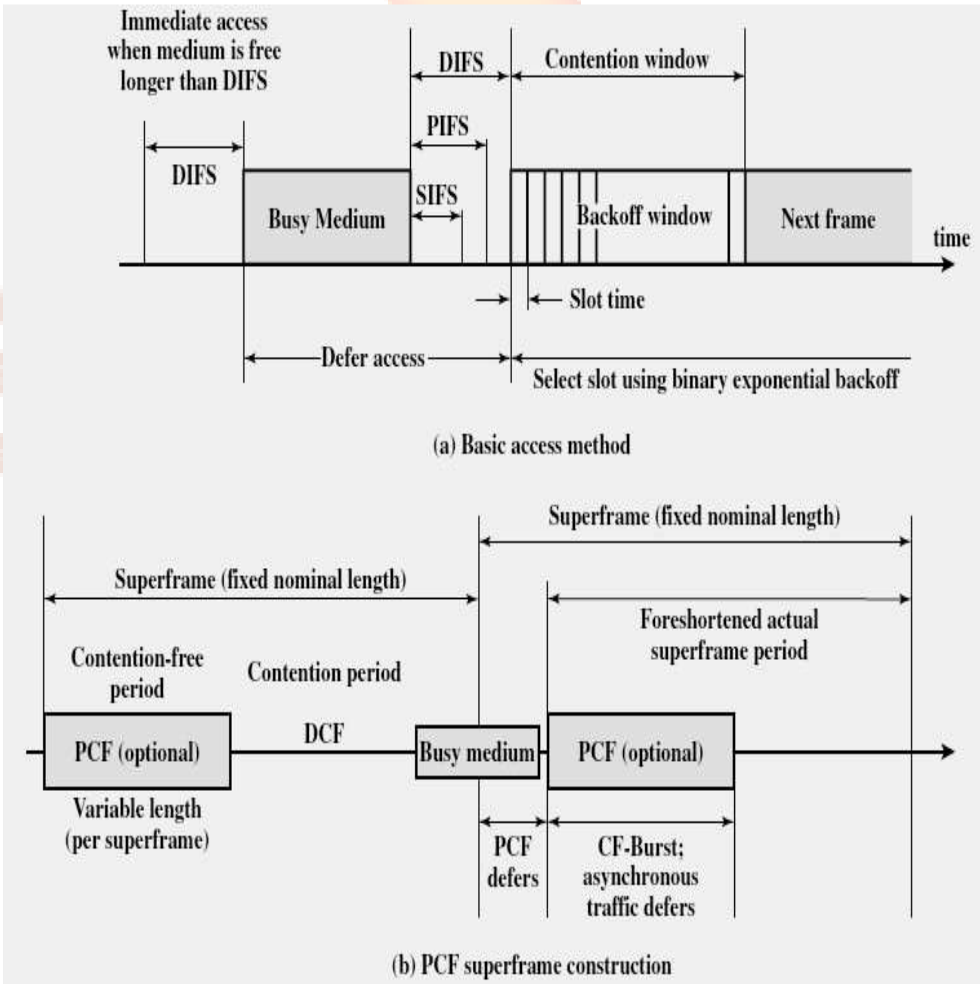

Fig 14.4: IEEE 802.11 MAC Timing

Any station using SIFS to determine transmission opportunity has the highest priority and the SIFS is used in the following circumstances:

- **Acknowledgment (ACK):** When a station receives a frame addressed only to itself, it responds with an ACK frame after waiting only for an SIFS gap. This has two desirable effects. First, because collision detection is not used, the likelihood of collisions is greater than with CSMA/CD, and the MAC-level ACK provides for efficient collision recovery. Second, the SIFS can be used to provide efficient delivery of an LLC protocol data unit (PDU) that requires multiple MAC frames. In this case, the following scenario occurs. A station with a multiframe LLC PDU to transmit sends out the MAC frames one at a time. Each frame is acknowledged by the recipient after SIFS. When the source receives an ACK, it immediately (after SIFS) sends the next frame in the sequence. The result is that once a station has contended for the channel, it will maintain control of the channel until it has sent all of the fragments of an LLC PDU.

- **Clear to Send (CTS):** A station can ensure that its data frame will get through by first issuing a small Request to Send (RTS) frame. The station to which this frame is addressed should immediately respond with a CTS frame if it is ready to receive. All other stations receive the RTS and defer using the medium.
- **Poll response:** This is explained in the discussion of PCF.

Point Coordination Function: PCF is an access method implemented on top of the DCF. The operation consists of polling by the centralized polling master (point coordinator). The point coordinator makes use of PIFS when issuing polls. Because PIFS is smaller than DIFS, the point coordinator can seize the medium and lock out all asynchronous traffic while it issues polls and receives responses. As an extreme, consider the following possible scenario. A wireless network is configured so that a number of stations with time-sensitive traffic are controlled by the point coordinator while remaining traffic contends for access using CSMA. The point coordinator could issue polls in a round-robin fashion to all stations configured for polling. When a poll is issued, the polled station may respond using SIFS. If the point coordinator receives a response, it issues another poll using PIFS. If no response is received during the expected turnaround time, the coordinator issues a poll.

If the discipline of the preceding paragraph were implemented, the point coordinator would lock out all asynchronous traffic by repeatedly issuing polls. To prevent this, an interval known as the superframe is defined. During the first part of this interval, the point coordinator issues polls in a round-robin fashion to all stations configured for polling. The point coordinator then idles for the remainder of the superframe, allowing a contention period for asynchronous access.

Figure 14.4(b) shows the use of the superframe. At the beginning of a superframe, the point coordinator may optionally seize control and issue polls for a given period. The remainder of the superframe is available for contention based access. At the end of the superframe interval, the point coordinator contends for access to the medium using PIFS. If the medium is idle, the point coordinator gains immediate access and a full superframe period follows. However, the medium may be busy at the end of a superframe. In this case, the point coordinator must wait until the medium is idle to gain access; this results in a foreshortened superframe period for the next cycle.

MAC Frame

Figure 14.5 shows the 802.11 frame format.

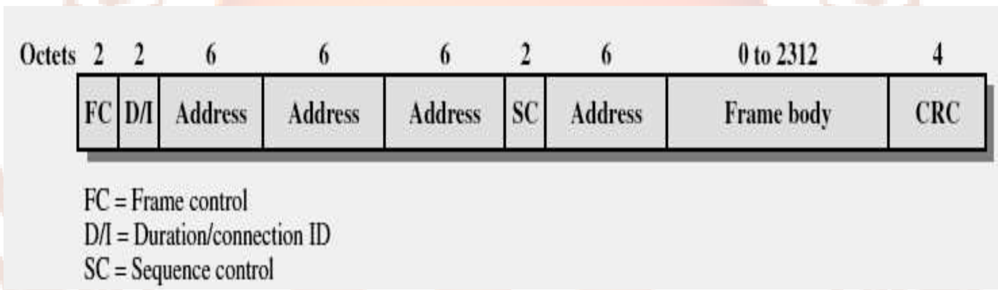

Fig 14.5: IEEE 802.11 MAC Frame Format

The fields are as follows:

- **Frame Control:** Indicates the type of frame (control, management, or data) and provides control information.
- **Duration/Connection ID:** If used as a duration field, indicates the time the channel will be allocated for successful transmission of a MAC frame. In some control frames, this field contains an association, or connection, identifier.
- **Addresses:** The number and meaning of the 48-bit address fields depend on context. The **transmitter address** and **receiver address** are the MAC addresses of stations joined to the BSS that are transmitting and receiving frames over the wireless LAN. The **service set ID** (SSID) identifies the wireless LAN over which a frame is transmitted. For an IBSS, the SSID is a random number generated at the time the network is formed. For a wireless LAN that is part of a larger configuration the SSID identifies the BSS over which the frame is transmitted; specifically, the SSID is the MAC-level address of the AP for this BSS (Figure 14.1). Finally, the **source address** and **destination address** are the MAC addresses of stations, wireless or otherwise, that are the ultimate source and

destination of this frame. The source address may be identical to the transmitter address and the destination address may be identical to the receiver address.

- **Sequence Control:** Contains a 4-bit fragment number subfield, used for fragmentation and reassembly, and a 12-bit sequence number used to number frames sent between a given transmitter and receiver.
- **Frame Body:** Contains an MSDU or a fragment of an MSDU. The MSDU is a LLC protocol data unit or MAC control information.
- Frame Check Sequence: **A 32-bit cyclic redundancy check.**

We now look at the three MAC frame types.

Control Frames: Control frames assist in the reliable delivery of data frames. There are six control frame subtypes:

- **Power Save-Poll (PS-Poll):** This frame is sent by any station to the station that includes the AP (access point). Its purpose is to request that the AP transmit a frame that has been buffered for this station while the station was in power saving mode.
- **Request to Send (RTS):** This is the first frame in the four-way frame exchange. The station sending this message is alerting a potential destination, and all other stations within reception range that it intends to send a data frame to that destination.
- **Clear to Send (CTS):** This is the second frame in the four-way exchange. It is sent by the destination station to the source station to grant permission to send a data frame.
- **Acknowledgment:** Provides an acknowledgment from the destination to the source that the immediately preceding data, management, or PS- Poll frame was received correctly.
- **Contention-Free (CF)-end:** Announces the end of a contention-free period that is part of the point coordination function.
- **CF-End + CF-Ack:** Acknowledges the CF-end. This frame ends the contention- free period and releases stations from the restrictions associated with that period.

Data Frames: There are eight data frame subtypes, organized into two groups. The first four subtypes define frames that carry upper-level data from the source station to the destination station. The four data-carrying frames are as follows:

- **Data:** It may be used in both a contention period and a contention-free period.

- **Data + CF-Ack:** May only be sent during a contention-free period. In addition to carrying data, this frame acknowledges previously received data.
- **Data + CF-Poll:** Used by a point coordinator to deliver data to a mobile station and also to request that the mobile station send a data frame that it may have buffered.
- **Data + CF-Ack + CF-Poll:** Combines the functions of the Data + CF- Ack and Data + CF-Poll into a single frame.

Management Frames: These frames are used to manage communications between stations and APs. Functions covered include management of associations (request, response, reassociation, dissociation, and authentication).

2.3 Addressing Mechanism

IEEE802.11 addressing mechanism specifies four cases, defined by the value of the two flags in the FC (frame control) field, to DS (distribution system) and from DS. Each flag can be either 0 or 1, which results in four different situations. The interpretation of the four addresses in the MAC frame depends on the value of these flags. Table 14.4 shows these addresses.

Table 14.4: Addresses

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

Address 1 is always the address of the next device. Address 2 is always the address of the previous device. Address 3 is the address of the final destination station if it is not defined by address 1. Address 4 is the address of the original source station if it is not the same as address 2. Here in first case where To DS and From DS is 00, the frame is not going to a distribution system (To DS=0) and is not coming from a distribution system (from DS=0). The frame is going from one station in a BSS to another without passing through the distribution system. Acknowledgement frame (ACK) should be sent to the original sender.

In the second case, To DS = 0 and From DS =1. This means that the frame is coming from a distribution system. The frame is coming from an AP and going to a station. The ACK should be sent to the AP. In the third case, To DS =1 and From DS =0. This means that the frame is going to a distribution system (To DS = 1). The frame is going from a station to an AP. The ACK is sent to the original station. Address 3 contains the final destination of the frame.

In case 4, To DS=1 and From DS =1. This is the case in which the distribution system is also wireless. The frame is going from one AP to another AP in a wireless distribution system. We do not need to define addresses if the distribution system is a wired LAN because the frame in these cases has the format of a wired LAN frame. We need four addresses to define the original sender, final destination and two intermediate APs.

2.4 Physical Layer

The physical layer for IEEE 802.11 has been issued in four stages. The first part, simply called IEEE 802.11, includes the MAC layer and three physical layer specifications, two in the 2.4-GHz band (ISM) and one in the infrared, all operating at 1 and 2 Mbps. IEEE 802.11a operates in the 5-GHz band at data rates up to 54 Mbps. IEEE 802.11b operates in the 2.4-GHz band at 5.5 and 11 Mbps. IEEE 802.11g also operates in the 2.4-GHz band, at data rates up to 54 Mbps. Table 14.5 provides details of IEEE 802.11 Physical Layer Standards.

Table 14.5: IEEE 802.11 Physical Layer Standards

	802.11	802.11a	802.11b	802.11g
Available bandwidth	83.5 MHz	300 MHz	83.5 MHz	83.5 MHz
Unlicensed frequency of operation	2.4–2.4835 GHz DSSS, FHSS	5.15–5.35 GHz OFDM 5.725–5.825 GHz OFDM	2.4–2.4835 GHz DSSS	2.4–2.4835 GHz DSSS, OFDM
Number of non-overlapping channels	3 (indoor/outdoor)	4 indoor 4 (indoor/outdoor) 4 outdoor	3 (indoor/outdoor)	3 (indoor/outdoor)
Data rate per channel	1, 2 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps	1, 2, 5.5, 11 Mbps	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
Compatibility	802.11	Wi-Fi5	Wi-Fi	Wi-Fi at 11 Mbps and below

Original IEEE 802.11 Physical Layer:

Three physical media are defined in the original 802.11 standard:

- **Direct sequence spread spectrum (DSSS)** operating in the 2.4-GHz ISM band, at data rates of 1 Mbps and 2 Mbps.
- **Frequency-hopping spread spectrum (FHSS)** operating in the 2.4- GHz ISM band, at data rates of 1 Mbps and 2 Mbps. The number of channels available ranges from 23 in Japan to 70 in the United States.
- Infrared at 1 Mbps and 2 Mbps operating at a wavelength between 850 and 950 nm

Direct Sequence Spread Spectrum: A DSSS system makes use of a chipping code, or pseudonoise sequence, to spread the data rate and hence the bandwidth of the signal. IEEE 802.11 DSSS uses the 11-chip Barker sequence. A **Barker sequence** is a binary {-1, +1} sequence {s(t)} of length n with the property that its autocorrelation values $R(\tau)$ satisfy $|R(\tau)|$ for all $|\tau| \le (n-1)$.

Frequency-Hopping Spread Spectrum

FHSS system makes use of a multiple channels, with the signal hopping from one channel to another based on a pseudonoise sequence. In the case of the IEEE 802.11 scheme, 1-MHz channels are used. For modulation, the FHSS scheme uses two-level Gaussian FSK for the 1-Mbps system. The bits zero and one are encoded as deviations from the current carrier frequency. For 2 Mbps, a four-level GFSK scheme is used, in which four different deviations from the center frequency define the four 2-bit combinations.

Infrared. The IEEE 802.11 infrared scheme is omnidirectional rather than point to point. A range of up to 20 m is possible. The modulation scheme for the 1-Mbps data rate is known as 16-PPM (pulse position modulation).

IEEE 802.11a

IEEE 802.11a makes use of the frequency band called the Universal Networking Information Infrastructure (UNNI), which is divided into three parts. The UNNI-1 band (5.15 to 5.25 GHz) is intended for indoor use; the UNNI-2 band (5.25 to 5.35 GHz) can be used either indoor or outdoor, and the UNNI-3 band (5.725 to 5.825 GHz) is for outdoor use. IEEE 80211.a has several advantages over IEEE 802.11b/g:

- IEEE 802.11a utilizes more available bandwidth than 802.11b/g. IEEE 802.11a provides much higher data rates than 802.11b and the same maximum data rate as 802.11g.
- IEEE 802.11a uses a different, relatively uncluttered frequency spectrum (5 GHz).

IEEE 802.11 does not use a spread spectrum scheme but rather uses orthogonal frequency division multiplexing (OFDM). In the case of OFDM, all of the sub channels are dedicated to a single data source. To complement OFDM, the specification supports the use of a variety of modulation and coding alternatives. The system uses up to 48 subcarriers that are modulated using BPSK, QPSK, 16-QAM, or 64-QAM.

Physical-Layer Frame Structure

The primary purpose of the physical layer is to transmit medium access control (MAC) protocol data units (MPDUs) as directed by the 802.11 MAC layer. The PLCP sublayer provides the framing and signaling bits needed for the OFDM transmission and the PDM sublayer performs the actual encoding and transmission operation. Figure 14.6(a) illustrates the physical layer frame format. The PLCP Preamble field enables the receiver to acquire an incoming OFDM signal and synchronize the demodulator. The Signal field, which consists of 24 bits encoded as a single OFDM symbol.

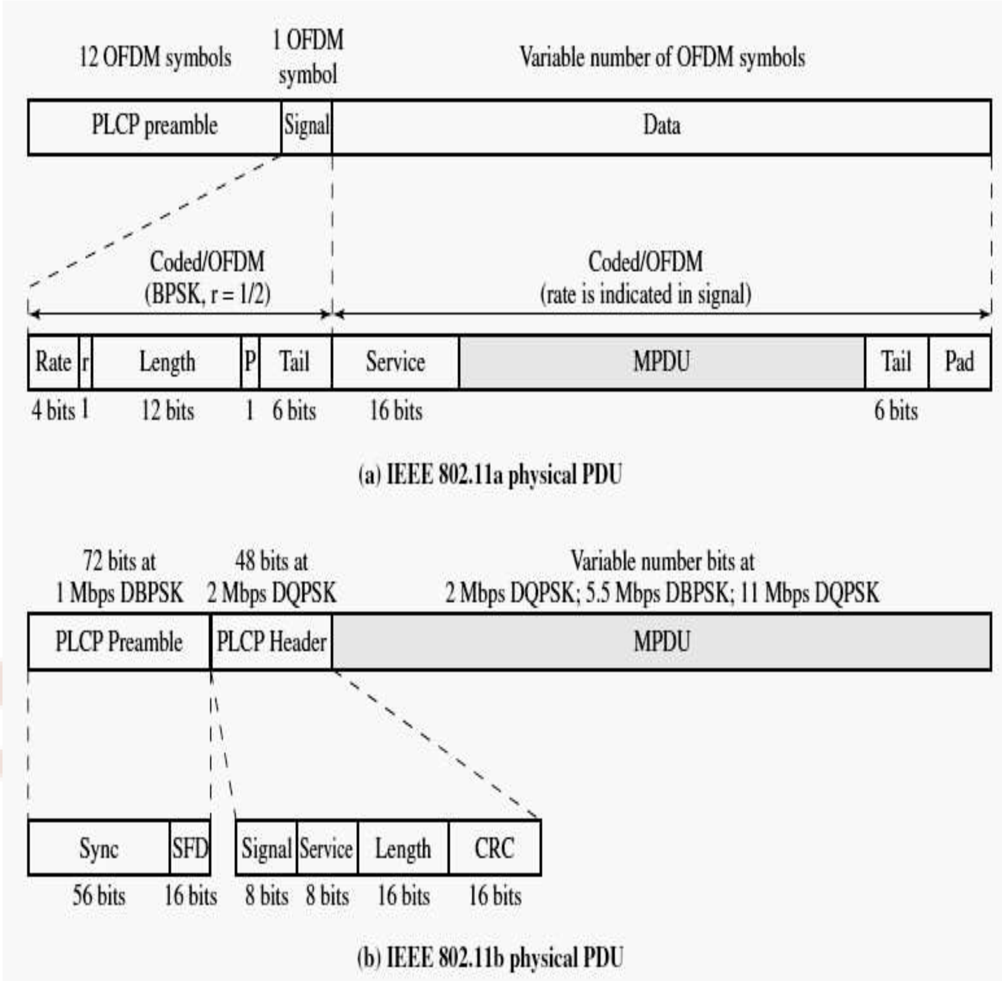

Fig 14.6: IEEE 802 Physical-Level Protocol Data Units

The Preamble and Signal fields are transmitted at 6 Mbps using BPSK. The signal field consists of the following subfields:

- **Rate:** Specifies the data rate at which the data field portion of the frame is transmitted
- **r:** reserved for future use
- **Length:** Number of octets in the MAC PDU
- **P:** An even parity bit for the 17 bits in the Rate, r, and Length subfields
- **Tail:** Consists of 6 zero bits appended to the symbol to bring the convolutional encoder to zero state

The **Data** field consists of a variable number of OFDM symbols transmitted at the data rate specified in the Rate subfield. The Data field consists of four subfields:

- **Service:** Consists of 16 bits, with the first 7 bits set to zeros to synchronize the descrambler in the receiver, and the remaining 9 bits (all zeros) reserved for future use.
- **MAC PDU:** Handed down from the MAC layer. The format is shown in figure 14.5.
- **Tail:** Produced by replacing the six scrambled bits following the MPDU end with 6 bits of all zeros; used to reinitialize the convolutional encoder.
- Pad: The number of bits required to make the Data field a multiple of the number of bits in an OFDM symbol (48, 96, 192, or 288).

IEEE 802.11b:

IEEE 802.11b is an extension of the IEEE 802.11 DSSS scheme, providing data rates of 5.5 and 11 Mbps in the ISM band. The chipping rate is 11 MHz, which is the same as the original DSSS scheme, thus providing the same occupied bandwidth. To achieve a higher data rate in the same bandwidth at the same chipping rate, a modulation scheme known as complementary code keying (CCK) is used. Figure 14.7 provides an overview of the scheme for the 11-Mbps rate.

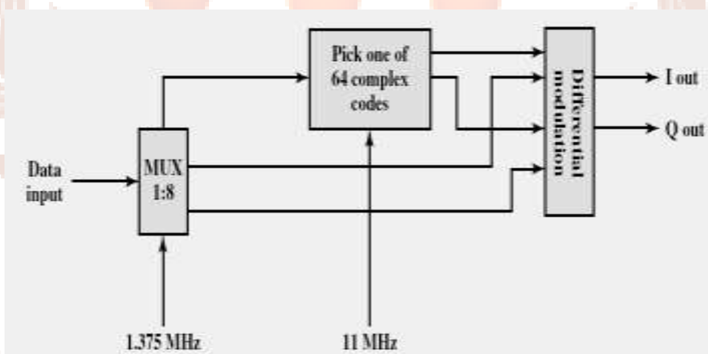

Fig 14.7: 11-Mbps CCK Modulation Scheme

Input data are treated in blocks of 8 bits at a rate of 1.375 MHz (8 bits/symbol * 1.375 MHz = 11 Mbps). Six of these bits are mapped into one of 64 codes sequences derived from a 64 * 64 matrix known as the ***Walsh matrix.*** The output of the mapping, plus the two additional bits, forms the input to a QPSK modulator.

IEEE 802.11b defines two physical-layer frame formats, which differ only in the length of the preamble. The long preamble of 144 bits is the same as used in the original 802.11 DSSS scheme and allows interoperability with other legacy systems. The short preamble of 72 bits provides improved throughput efficiency. Figure 14.9b shows the physical layer frame format with the short preamble. The **PLCP Preamble** field enables the receiver to acquire an incoming signal and synchronize the demodulator. It consists of two subfields: a 56-bit **Sync** field for synchronization, and a 16-bit start-of- frame delimiter **(SFD).** The preamble is transmitted at 1 Mbps using differential BPSK and Barker code spreading.

Following the preamble is the **PLCP Header,** which is transmitted at 2 Mbps using DQPSK. It consists of the following subfields:

- **Signal**: Specifies the data rate at which the MPDU portion of the frame is transmitted.
- **Service:** Only 3 bits of this 8-bit field are used in 802.11b. One bit indicates whether the transmit frequency and symbol clocks use the same local oscillator. Another bit indicates whether CCK or PBCC encoding is used. A third bit acts as an extension to the Length subfield.
- **Length:** Indicates the length of the MPDU field by specifying the number of microseconds necessary to transmit the MPDU.
- **CRC:** A 16-bit error detection code used to protect the Signal, Service, and Length fields.

The MPDU field consists of a variable number of bits transmitted at the data rate specified in the Signal subfield. Prior to transmission, all of the bits of the physical layer PDU are scrambled.

IEEE 802.11g

IEEE 802.11g extends 802.11b to data rates above 20 Mbps, up to 54 Mbps. Like 802.11b, 802.11g operates in the 2.4-GHz range and thus the two are compatible. The standard is designed so that 802.11b devices will work when connected to an 802.11g AP, and 802.11g devices will work when connected to an 802.11b AP, in both cases using the lower 802.11b data rate.

SELF ASSESSMENT QUESTIONS – 1

1. IEEE has defined the specifications for a wireless LAN, called ______________________.
2. "The first 802.11 standard to gain broad industry acceptance was 802.11b". State true or false.

   (a) True (b) False
3. The term used for certified 802.11b products is______________________.
4. The smallest building block of a wireless LAN is______________________.
5. When all the stations in the BSS are mobile stations, with noconnection to other BSSs, the BSS is called__________________________________.
6. ______________ consists of two or more basic service sets interconnected by a distribution system.
7. To integrate the IEEE 802.11 architecture with a traditional wired LAN,a ____________________is used.
8. The two services involved with the distribution of messages within a DS are____________________and______________________.

3. BLUETOOTH

In 1994, the L. M. Ericsson company became interested in connecting its mobile phones to other devices (e.g., PDAs) without cables. Together with four other companies (IBM, Intel, Nokia, and Toshiba), it formed a SIG (Special Interest Group, i.e., consortium) to develop a wireless standard for interconnecting computing and communication devices and accessories using short-range, low-power, inexpensive wireless radios. The project was named Bluetooth, after Harald Blaatand, the king of Denmark (940-981) who united Denmark and Norway. Blaatand translates to Bluetooth in English.

Today, bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard. The standard defines a wireless personal-area network (PAN) operable in an area the size of a room or hall. Bluetooth technology has several applications. Peripheral devices such as a wireless mouse or keyboard can communicate with the computer through this technology. Monitoring devices can communicate with sensor devices in a small health care centre. Home security devices use this technology to connect different sensors to the main security controller.

3.1 Bluetooth Architecture

The basic unit of a Bluetooth system is a piconet, which consists of a master node and up to seven active slave nodes within a distance of 10 meters. Multiple piconets can exist in the same (large) room and can even be connected via a bridge node. An interconnected collection of piconets is called a scatternet. A piconet can have up to eight stations, one of which is called primary and rest are called secondaries. All secondary stations synchronize their clocks and hopping sequence with primary. A piconet can have only one primary station. The communication between primary and secondary can be one to one or one to many. Figure 14.8 shows a piconet.

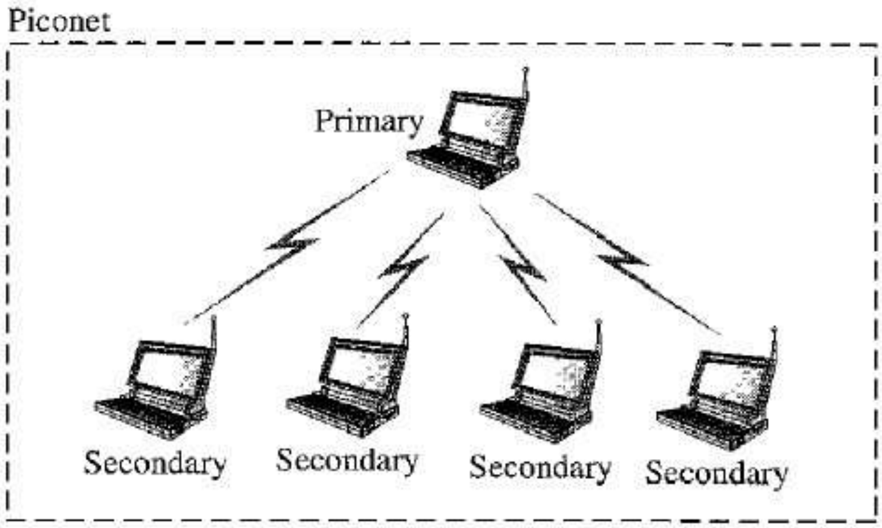

Fig 14.8: Piconet

Although a piconet can have a maximum of seven secondaries, an additional eight secondaries can be in the parked state. A secondary in a parked state is synchronized with primary but cannot take part in communication until it is moved from the parked state. Because only eight stations can be active in a piconet, activating a station from the parked state means that an active station must go to the parked state.

Piconets can be combined to form scatternet. A secondary station in one piconet can be the primary in another piconet. The station can receive messages from the primary in the first piconet and acts as a primary, deliver them to secondaries in the second piconet. A station can be a member of two piconets. Figure 14.9 shows a scatternet.

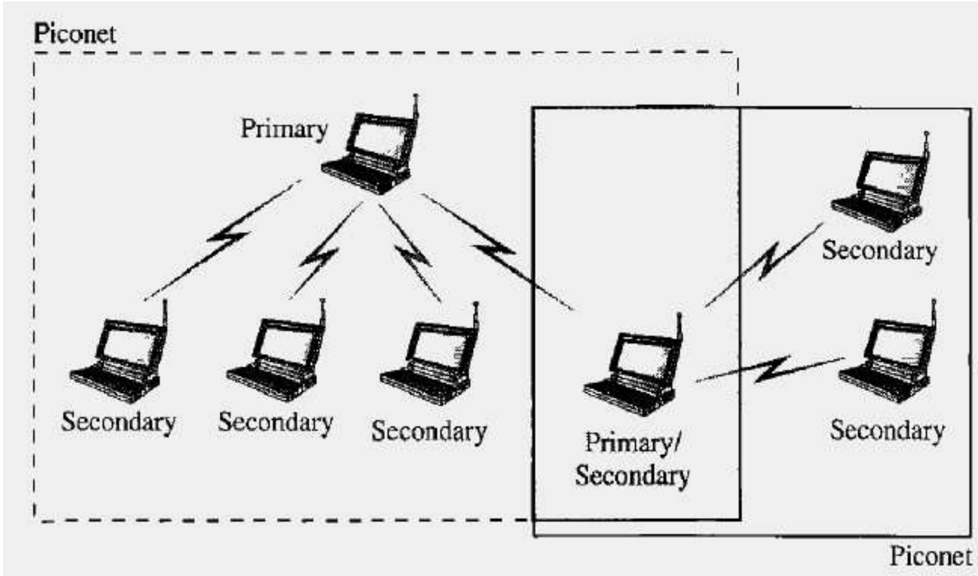

Fig 14.9: Scatternet

A bluetooth device has a built in short range radio transmitter. The current data rate is 1 Mbps with 2.4GHz bandwidth.

3.2 Bluetooth Layers

Bluetooth uses several layers. Figure 14.10 shows these layers.

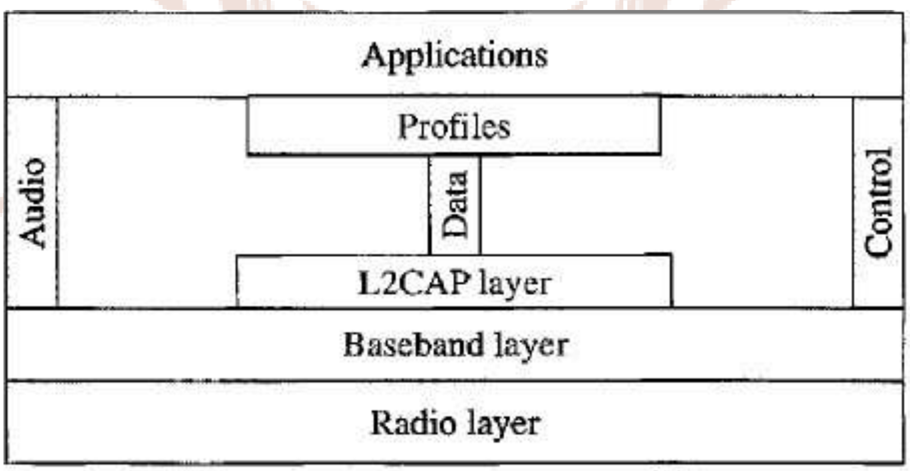

Fig 14.10: Bluetooth Layers

Radio Layer

The radio layer is roughly equivalent to the physical layer of the internet model. Bluetooth devices are low-power and have a range of 10m.

Baseband Layer

The baseband layer is roughly equivalent to the MAC sublayer in LANs. The access method is TDMA (time division multiple access). The primary and secondary communicate with each other using time slots. The length of the time slot is exactly same as the dwell time, 625 μs. this means that during the time that one frequency is used, a sender sends a frame to secondary or secondary sends a frame to primary. The communication is only between the primary and secondary. Secondaries cannot communicate directly with one another.

L2CAP

The logical Link Control and Adaptation Protocol (L2CAP) is roughly equivalent to the LLC sublayer in LANs. It is used for data exchange on an ACL (asynchronous connectionless link) link. SCO (synchronous connection oriented) channels do not use L2CAP. Figure 14.11 shows the format of the data packet at this level.

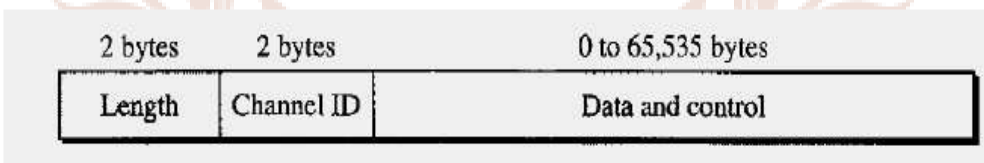

Fig 14.11: L2CAP data packet format

The 16 bit field defines the size of the data in bytes coming from upper layers. Data can be up to 65,535 bytes. The channel ID defines a unique identifier for the virtual channel created at this level.

The L2CAP has specific duties such as multiplexing, segmentation and reassembly, quality of service and group management.

Other Upper Layers

Bluetooth defines several protocols for the upper layers that use the services of L2CAP; these protocols are specific for each purpose.

SELF ASSESSMENT QUESTIONS – 2

9. The L. M. Ericsson company together with four other companies formed a____________to develop a wireless standard for interconnecting computing and communication devices.
10. The bluetooth project was named after_______.
11. Today, bluetooth technology is the implementation of a protocoldefined by the________standard.
12. The basic unit of a Bluetooth system is a___________________.
13. An interconnected collection of piconets is called a________________.
14. Which layer of the internet model is closely related to radio layer?
    a) Physical layer
    b) Network layer
    c) Application layer
    d) Data link layer
15. Bluetooth devices are low-power and have a range of ___________ meter.
16. The baseband layer is roughly equivalent to the______________sublayerin LANs.

4. SUMMARY

Let us recapitulate the important concepts discussed in this unit:

- IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data link layers.
- Basic service set (BSS), is the smallest building block of a wireless LAN.
- When all the stations in the BSS are mobile stations, with no connection to other BSSs, the BSS is called an independent BSS (IBSS).
- An extended service set (ESS) consists of two or more basic service sets interconnected by a distribution system.
- The IEEE 802.11 MAC layer covers three functional areas: reliable data delivery, access control, and security.
- In 1994, the L. M. Ericsson company together with four other companies (IBM, Intel, Nokia, and Toshiba), it formed a SIG (Special Interest Group, i.e., consortium) to develop a wireless standard for interconnecting computing and communication devices and accessories using short-range, low-power, inexpensive wireless radios.
- The basic unit of a bluetooth system is a piconet, which consists of a master node and up to seven active slave nodes within a distance of 10 meters.
- An interconnected collection of piconets is called a scatternet.
- The L2CAP has specific duties such as multiplexing, segmentation and reassembly, quality of service and group management.

5. TERMINAL QUESTIONS

1. Explain IEEE802.11 architecture.
2. Explain the functions of IEEE medium access control sublayer.
3. Describe IEEE802.11 addressing mechanism.
4. Describe bluetooth architecture.
5. Explain bluetooth layers.

6. ANSWERS

Self-Assessment Questions

1. IEEE802.11
2. (a) True
3. Wi-Fi
4. Basic service set (BSS)
5. Independent BSS
6. Extended service set (ESS)
7. Portal
8. Distribution, integration
9. SIG (Special Interest Group)
10. Harald Blaatand
11. IEEE 802.15
12. Piconet
13. Scatternet
14. (a) physical layer
15. 10 meter
16. Medium Access Control (MAC)

Terminal Questions

1. In 1990, the IEEE 802 Committee formed a new working group, IEEE 802.11, specifically devoted to wireless LANs, with a charter to develop a MAC protocol and physical medium specification. (Refer section 2.1 for detail).

2. The IEEE 802.11 MAC layer covers three functional areas: reliable data delivery, access control, and security. Let see the first two topics in this section. (Refer section 2.2 for detail).
3. IEEE802.11 addressing mechanism specifies four cases, defined by the value of the two flags in the FC (frame control) field, to DS (distribution system) and from DS. (Refer section 2.3 for detail).
4. The basic unit of a Bluetooth system is a piconet, which consists of a master node and up to seven active slave nodes within a distance of 10 meters. Multiple piconets can exist in the same (large) room and can even be connected via a bridge node. (Refer section 3.1 for detail).
5. Bluetooth uses several layers such as radio layer, baseband layer, L2Cap layer etc. (Refer section 3.2 for detail)

References:

1. Behrouz A. Forouzan, Sophia Chung Fegan, “Data Communications and Networking”, Fourth edition.
2. William Stallings, “Data and Computer Communications”, Sixth edition, Pearson Education, Delhi, 2002.
3. Taub and Schilling, “Principles of Communication Systems”, Tata Mc Graw Hill, Delhi, 2002.
4. S. Tanenbaum, ”Computer Networks”, Pearson Education, Fourth Edition.
5. N. Olifer, V. Olifer, ”Computer Networks: Principles, technologies and Protocols for Network design”, Wiley India Edition, First edition.
6. Simon Poulton (2003), packet switching and X.25 Networking, Pitman publishing.
7. Walrand, P.Varaiya, “high performance communication networks”, Morgan kaufmann.