UNIT II

2 Wireless Standards

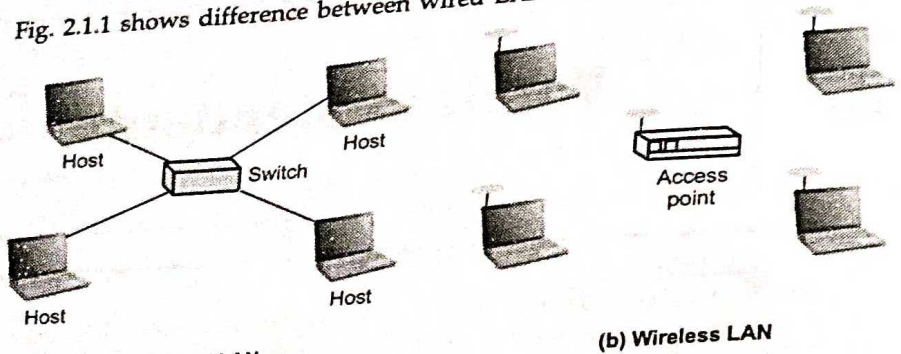
Syllabus

Wireless LANs : *Fundamentals of WLAN, Design goals, Characteristics, Network Architecture, IEEE 802.11: components in IEEE 802.11 network, Physical Layer,* ***MAC Sub Layers :*** *DCF, PCF, Hidden and exposed station problem, Frame format, Addressing Mechanism, IEEE 802.15.1* ***Bluetooth :*** *Architecture Layers, operational states,* ***IEEE 802.16 WiMax :*** *Services, Architecture, Layers, comparison between Bluetooth, IEEE 802.11 and IEEE 802.16.*

Contents

2.1 Wireless LANs

- Fig. 2.1.1 shows difference between wired LAN and wireless LAN.



(a) Wired LAN (b) Wireless LAN

Fig. 2.1.1

- Wired LAN uses cables to connect host and wireless LAN uses radio frequencies. Wired LAN uses hub and switch for designing network. Wireless LAN uses access point for designing network.
- Wired LAN : Networks are invisible to other wired networks. The presence of one wired network has no effect on the performance of another wired network. All of the nodes on a wired network can hear all other nodes.
- Wireless LAN : Wireless networks are often visible to other wireless networks. One wireless network can affect the performance of other wireless networks. Many nodes on a wireless network cannot hear all of the other wireless nodes on the same network.
- Access method : Wired LAN uses CSMA/CD and wireless LAN uses CSMA/CA.
- The CSMA/CD algorithm does not work in wireless LANs for three reasons :
  1. Wireless hosts do not have enough power to send and receive at the same time.
  2. The hidden station problem prevents collision detection.
  3. The distance between stations can be great.
- Bandwidth supported by wired LAN is 100 Mbps and wireless LAN is 54 Mbps (IEEE 802.11).

2.1.1 WLAN Design Goals

- Design goals are listed below :
  1. Support for global, seamless operation.
  2. Low power for battery use.

  3. No special permissions or licenses required to use the LAN.
  4. Robust transmission technology.
  5. Easy to use for everyone, simple management.
  6. Security : No one should be able to read sensitive data.
  7. Privacy : No one should be able to collect user profiles.

2.1.2 Applications of WLAN

1. **LAN extension :**
   - A wireless LAN saves the cost of the installation of LAN cabling and eases the task of relocation and other modifications to network structure.
2. **Cross building interconnect :**
   - To connect the LAN in nearby buildings, they can be wired or wireless LANs. A point-to-point wireless link is used between two buildings.
3. **Nomadic access :**
   - It provides a wireless link between a LAN hub and a mobile data terminal equipped with an antenna.
4. **Ad hoc networking :**
   - An Ad hoc network is peer-to-peer network set up temporarily to meet some immediate need.
5. Network managers in dynamic environments minimize the cost of moves, network extensions, and other changes by eliminating the cost of cabling and installation.
6. Network managers in older buildings, such as schools, hospitals, and warehouses, find WLANs to be a most cost-effective infrastructure solution.
7. In business, people can work productively with customers or suppliers in meeting rooms - There is no need to leave the room to check if important emails have arrived or print big files.

2.1.3 Requirements of Wireless LAN

- Important requirement for Wireless LAN are as follows. These are also called as **properties of wireless LAN.**
  1) Number of nodes
  2) Throughput
  3) Connection to backbone LAN
  4) Service area
  5) Battery power consumption

6) Transmission robustness and security

7) License free operation

8) Hand off/roaming

9) Dynamic configuration.

2.1.4 WLAN Network Architecture

- WLAN is of two types :

1. Infrastructure network 2. Ad-hoc LAN

Architecture of an infrastructure network

- Fig. 2.1.2 shows architecture of an infrastructure network.

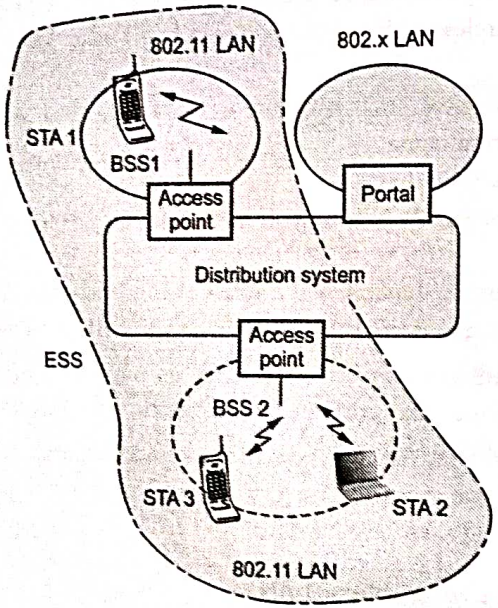


Fig. 2.1.2 Architecture of an infrastructure network

1. Station (STA) : Terminal with access mechanisms to the wireless medium and radio contact to the access point.
2. Basic Service Set (BSS) is a group of stations using the same radio frequency.
3. Access point is a station integrated into the wireless LAN and the distribution system.
4. Portal is used to bridge to other wired networks. A portal is the logical integration between wired LANs and 802.11. It also can serve as the access point to the DS.

- All data going to an 802.11 LAN from an 802.X LAN must pass through a portal. It thus functions as bridge between wired and wireless.
- Distribution system : Interconnection network to form one logical network based on several BSS. Distribution system services includes : Association, re-association, disassociation, distribution and integration.
- Distribution is the primary service used by IEEE 802.11 STAs. It is conceptually invoked by every data message to or from an IEEE 802.11 STA operating in an ESS.
- The implementation of the DS is not specified by 802.11. Therefore, a distribution system may be created from existing or new technologies.
- A point-to-point bridge connecting LANs in two separate buildings could become a DS.
- Extended service set : A set of one or more interconnected BSS's and integrated LANs that (ESS) appear as a single BSS to the LLC layer at any station associated with one of these BSS's.

2.1.5 IEEE 802.11 Services

- There are five services provided by IEEE 802.11 :

1. Association 2. Reassociation
3. Disassociation 4. Distribution
5. Integration.

- The first three services (Association, re-association and disassociation) is deal with station mobility.

1. Association

- Before a STA is allowed to send a data message via an AP, it first becomes associated with the AP.
- The act of becoming associated invokes the association service, which provides the STA to AP mapping to the DS. The DS uses this information to accomplish its message distribution service.
- Association is sufficient to support no transition mobility. Association is one of the services in the DSS.

2. Reassociation

- This service allows the station to switch its association from one access point to another.
- Both association and reassociation are initiated by the station.

3. Disassociation

- Disassociation is when the association between the station and the AP is terminated. This can be initiated by either party.
- A disassociated station cannot send or receive data. ESS-transition is not supported. A station can move to a new ESS but will have to reinitiate connections.
- The MAC management facility protects itself against stations that disappear without notification.

4. Distribution and Integration

- Distribution is simply getting the data from the sender to the intended receiver.
- The message is sent to the local access point and then distributed through the DS to the output AP that the recipient is associated with.
- If the sender and receiver are in the same BSS, the input and out AP's are the same. So the distribution service is logically invoked whether the data is going through the DS or not.
- Integration is when the output AP is a portal. Thus, 802.x LANs are integrated into the 802.11 DS.

2.1.6 Advantages and Disadvantages of Wireless LANs

Advantages

1. Very flexible within the reception area
2. Ad-hoc networks without previous planning possible
3. No wiring difficulties (e.g. historic buildings, firewalls)
4. More robust against disasters like, e.g., earthquakes, fire - or users pulling a plug.

Disadvantages

1. Typically very low bandwidth compared to wired networks (1-10 Mbit/s)
2. Many proprietary solutions, especially for higher bit-rates, standards take their time (e.g. IEEE 802.11)
3. Products have to follow many national restrictions if working wireless, it takes a vary long time to establish global solutions like, e.g., IMT-2000.

2.1.7 Comparison of IEEE 802.3 and IEEE 802.11

Sr. No.	IEEE802.3 (Wired LAN)	IEEE 802.11 (WLAN)
1.	IEEE standard 802.3.	IEEE standard 802.11.
2.	Communication medium is co-axial cable.	Infrared or radio frequencies act as medium.
3.	Spread spectrum is not used.	Spread spectrum is used.
4.	It uses MAC.	It uses two MAC sub-layers.
5.	802.3 frames have only a Source Address (SA) and Destination Address (DA).	802.11 frames have up to four address fields in the MAC header. Source Address (SA), Destination Address (DA), Transmitter Address (TA), Receiver Address (RA).
6.	It uses CSMA/CD.	It uses CSMA/CA.
7.	LANs suffer less interference as electric signals travel using cables.	WLANs suffer from interference of various types during travel from source to the destination.
8.	The efficiency is high.	The efficiency is low.
9.	Addressing is simpler.	Addressing is complicated.
10.	It has a large range.	It has a short range.
11.	Ethernet supports full duplex mechanism for communication when a switch connects using a single device rather than hub.	WLAN uses half duplex mechanism for communication.
12.	Data payload 1,500 bytes.	Data payload 2,304 bytes.

2.2 IEEE 802.11

SPPU : Dec.-14,15,16, May-15,16,17

- Wireless networks have many applications. For example, user on the road often want to use their laptop to send and receive faxes, telephone calls, electronic mails, read remote files, login on remote machines and so on. Wireless networks use unguided media for transmission and reception are achieved by means of an antenna. The atmosphere and outer space are the examples of unguided media that provide a means of transmitting electromagnetic signals but do not guide them. This form of transmission is usually referred to as **wireless transmission**. For transmission, the antenna radiates electromagnetic energy into the media and for reception, the antenna picks up electromagnetic waves from the surrounding medium.

- There are basically two types of configurations for wireless transmission : directional and omnidirectional. In directional configuration, the transmitting antenna puts out a focused electromagnetic beam; the transmitting and receiving antenna must therefore be carefully aligned. In the omnidirectional case, the transmitted signal spreads out in all directions and can be received by many antennas. In general, the higher the frequency of a signal, the more it is possible to focus it into a directional beam.
- When a wireless LAN terminal is to install with a wired network (ethernet), a base station with antenna is necessary. Also, when all the terminals are a part of wireless LAN, the base station is not required.
- IEEE 802-11 protocol supports both the types of configuration.

2.2.1 IEEE 802.11x

- 802.11 refer to a family of specifications developed by the IEEE for wireless LAN technology. There are three specifications in the family : 802.11, 802.11a and 802.11b. All three of the specifications use Carrier Sense Multiple Access with Collision Detection (CSMA/CD) as the path sharing protocol. Specifications of 802.11 family :

1. 802.11 - It is wireless LAN and provides 1 Mbps or 2 Mbps transmission in the 2.4 GHz band. It uses Frequency Hopping Spread Spectrum (FHSS) or Direct Sequence Spread Spectrum (DSSS).

2. 802.11a - It provides upto 54 Mbps in the 5 GHz band. It uses orthogonal frequency division multiplexing encoding scheme.

3. 802.11b - It also refers to Wi-Fi. It provides 11 Mbps transmission in the 2.4 GHz band. 802.11b uses only direct sequence spread spectrum.

4. 802.11g - It provides 20 Mbps and more in the 2.4 GHz band.

- 802.11 LAN is based on a cellular architecture. The system is subdivided into cell. Each cell is controlled by a base station. Cell is called as Basic Service Set (BSS) and base station is Access Point (AP). Wireless LAN may be formed by a single cell, with a single access point. Fig. 2.2.1 shows the typical 802.11 LAN. (See Fig. 2.2.1 on next page.)
- Set of BSS can be interconnected by a distribution system to form an Extended Service Set (ESS). BSS are like cells in a cellular network. Each BSS has an access point. An ESS can also provide gateway access for wireless users into a wired network such as the internet. The standard also defines the concept of a portal.

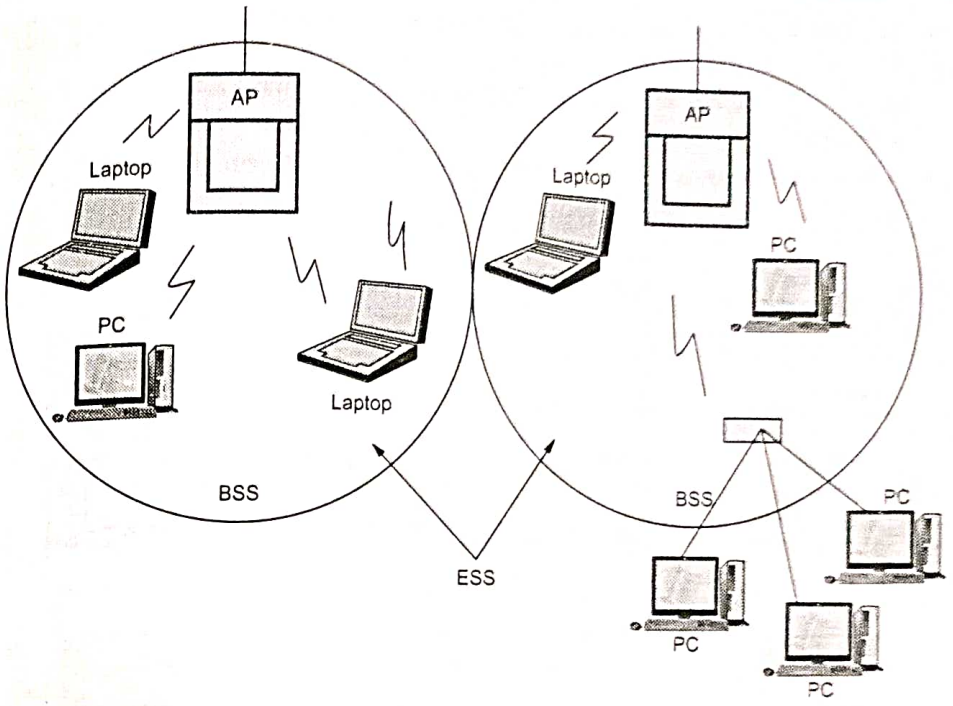


Fig. 2.2.1 802.11 LAN

Portal is a device that interconnects between an 802.11 and another 802LAN. IEEE 802.11 architecture consists of ,

1. Distribution System (DS)
2. Access Point (AP)
3. Basic Service Set (BSS)
4. Extended Service Set (ESS).

2.2.2 IEEE 802.11 Architecture

- IEEE 802.11 standard defines two types of services.
  a. Basic Service Set (BSS)
  b. Extended Service Set (ESS)
- The Basic Service Set (BSS) is the basic building block of the IEEE 802.11 architecture. A BSS is defined as a group of stations that co-ordinates their access to the medium under a given instance of the medium access control. Each BSS has an **Access Point** (AP) that has station functionality and provide access to the distributed system.

- The BSS without an AP is a stand-alone network and cannot send data to other BSS. A single BSS can be used to form an Ad hoc network. An Ad hoc network consists of a group of stations within range of each other. Ad hoc network are typically temporary in nature.
- A BSS with an AP is sometimes referred to as an infrastructure network. Fig. 2.2.2 shows the BSS.

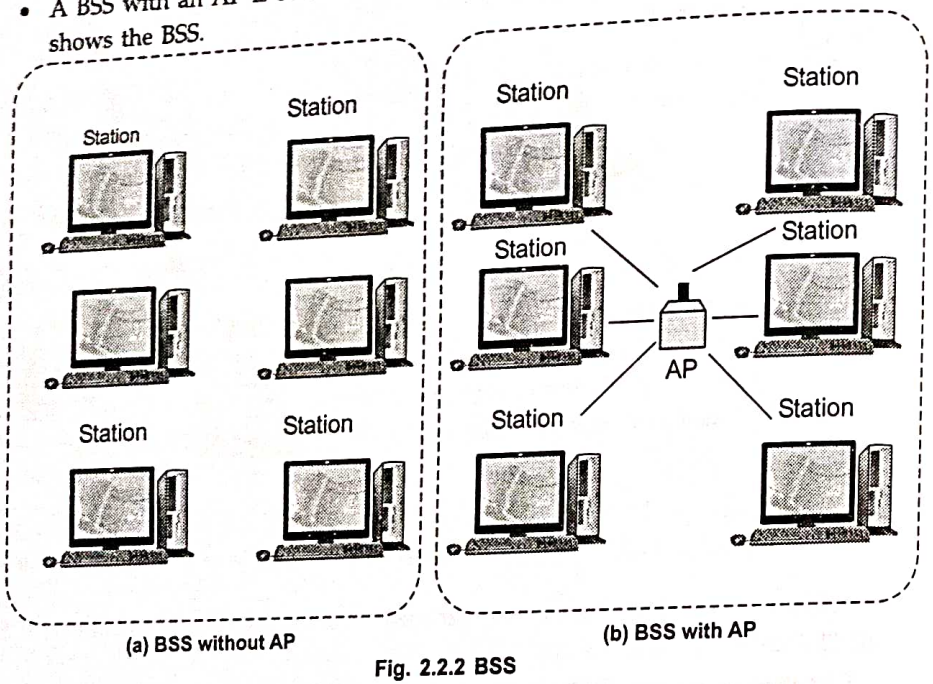


Fig. 2.2.2 BSS

Extended Service Set (ESS)

Refer Fig. 2.2.3 on next page.

- A set of BSS can be interconnected by a distribution system to form an extended service set. An ESS can also provide gateway access for wireless users into a wired network such as the Internet.
- ESS uses two types of stations : Mobile and stationary. The mobile stations are normal stations inside a BSS. The stationary stations are AP stations that are part of a wired LAN. Fig. 2.2.3 shows an ESS.
- The distribution system provides the distribution service, which is,

1. The transfer of MAC Service Data Unit (SDU) between APs of BSS within the ESS.
2. The transfer of MSDU between portals and BSS within the ESS.
3. The transport of MSDU between stations in the same BSS when either the MSDU has a multicast or broadcast address or the sending station chooses to use the distribution service.

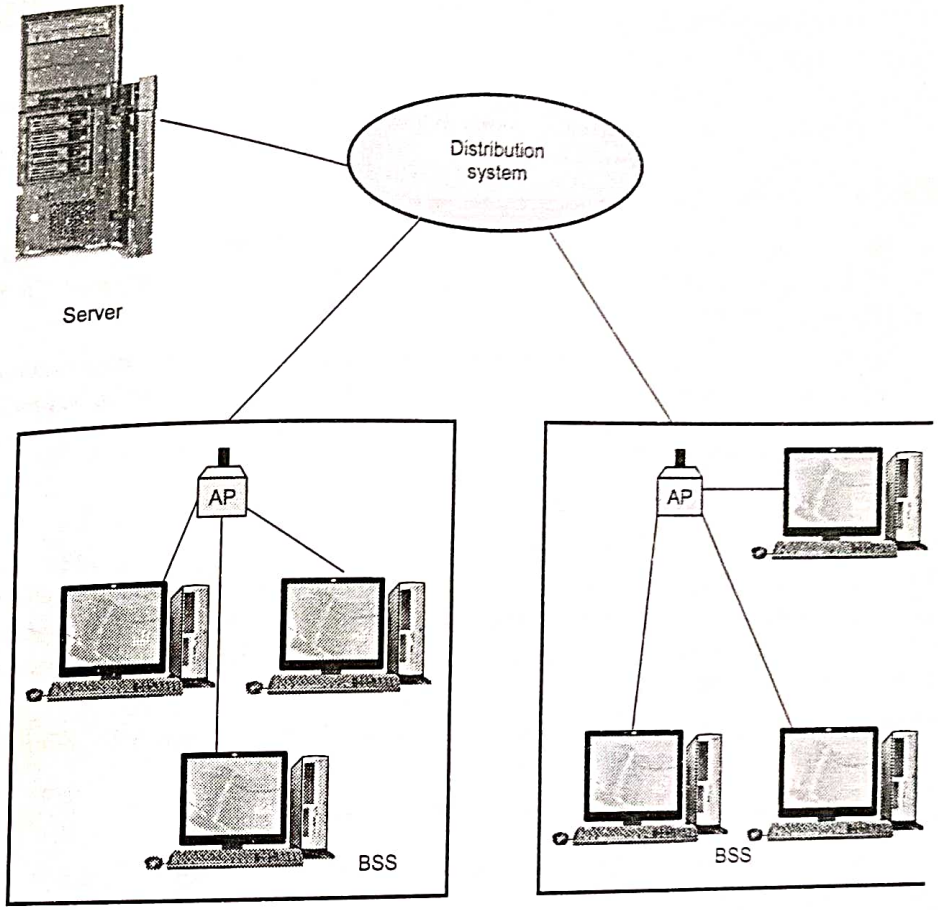


Fig. 2.2.3 ESS

- The role of the distribution service is to make the ESS appear as a single BSS to the LLC that operate above the medium access control in any of the stations in the ESS.
- IEEE 802.11 defines the distribution service but not the distribution system. The distribution system can be implemented by using wired or wireless networks.

Types of stations

- IEEE 802.11 defines three types of stations based on their mability in a wireless LAN.

  1. No-transition 2. BSS-transition 3. ESS-transition.

- A station with no-transition mobility is either stationary or moving only inside a BSS.

- A station with BSS-transition mobility can move from one BSS to another, but the movement is confined inside one ESS.
- A station with ESS-transition mobility can move from one ESS to another. The IEEE 802.11 does not guarantee the communication is continuous during the move.

2.2.3 MAC Sublayer

- MAC sublayer is responsible for the channel access procedures, Protocol Data Unit (PDU) addressing, frame formatting, error checking and fragmentation and reassembly of MSDUs.
- MAC layer also provides options to spport security service through authentication and privacy mechanisms. MAC management service are also defined to support roaming within an ESS and to assist stations in power management.
- IEEE 802.11 defines two MAC sublayers :
  1. Distributed Co-ordination Function (DCF)
  2. Point Co-ordination Function (PCF).
- The DCF provides support for asynchronous data tranfer of MSDU on a best effort basis. Under this function, the transmission medium operates in the contention mode exclusively, requiring all stations to contend for the channel for each packet transmitted.
- PCF may be implemented by an AP, to support connection-oriented time-bounded transfer of MSDU.
- Fig. 2.2.4 shows the MAC layers in IEEE 802.11 standard.

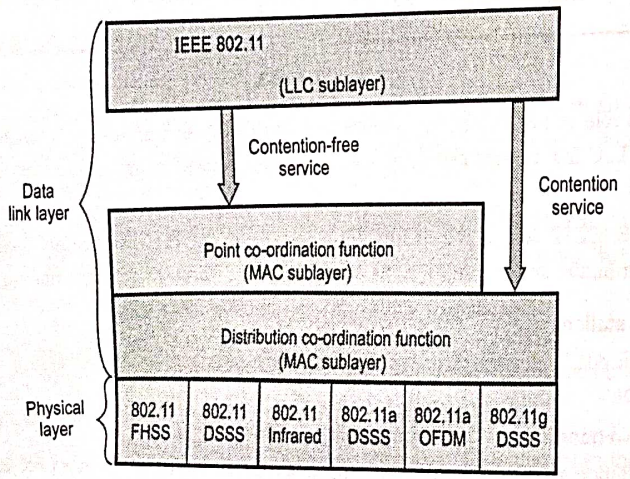


Fig. 2.2.4 IEEE 802.11 MAC layer

2.2.3.1 Distributed Co-ordination Function (DCF)

- The DCF is the basic access method used to support asynchronous data transfer on a best effort basis. All stations are required to support the DCF. The access control in ad hoc networks use only the DCF.
- The DCF is based on the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol. Carrier sensing involves monitoring the channel to determine whether the medium is idle or busy.
- Wireless LAN cannot implement CSMA/CD for three reasons :
  1. For collision detection a station must be able to send data and receive collision signals at the same time.
  2. Collision may not be detected because of the hidden station problem.
  3. The distance between station can be great signal fading could prevent a station at one end from hearing a collision at the other end.
- The DCF interframe space is used by the DCF to transmit data and management MDPUs. Fig. 2.2.5 shows the exchange of data and control frames in time.

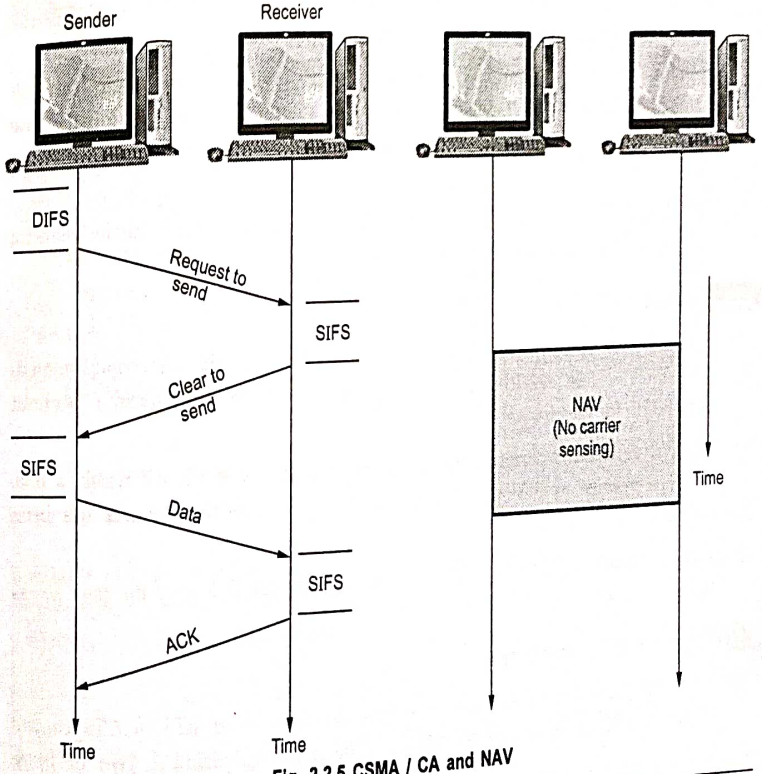


Fig. 2.2.5 CSMA / CA and NAV

1. Before sending a frame, the source station senses the medium by checking the energy level at the carrier frequency.

a. The channel uses a persistence strategy with back off until the channel is idle.

b. After the station is found to be idle, the station waits for a period of time called the Distributed Interframe Space (DIFS); then the station sends a control frame called the Request To Send (RTS).

2. After receiving the RTS and waiting a period of time called the Short Interframe Space (SIFS), the destination station sends a control frame, called the Clear To Send (CTS), to the source station. This control frame indicates that the destination station is ready to receive data.

3. The source station sends data after waiting an amount of time equal to SIFS.

4. The destination station, after waiting an amount of time equal to SIFS, sends an acknowledgement to show that the frame has been received.

- The source station set the **duration field** in the MAC header of data frames or in RTS and CTS control frames. The **duration field** indicates the amount of time after the end of the present frame that the channel will be utilized to complete the successful transmission of the data or management frame.
- Stations detecting a duration field in a transmitted MSDU adjust their **Network Allocation Vector (NAV)**, which indicates the amount of time that must elapse until the current transmission is complete and the channel can be sampled again for idel status.
- The channel is marked busy if either the physical or virtual carrier sensing mechanism indicates that the channel is busy.

2.2.3.2 Point Co-ordination Function (PCF)

- The PCF is an optional capability that can be used to provide connection oriented, contention - free services by enabling polled stations to transmit without contending for the channel.
- The PCF function is performed by the point co-ordinator in the AP within a BSS. To give priority to PCF over DCF, another set of interframe spaces has been defined : PIFS and SIFS.
- Due to priority of PCF over DCF, stations that only use DCF may not gain access to the medium.

2.2.3.3 Collision during Handshaking

- What happens if there is collision during the time when RTS or CTS control frames are in transition, often called the handshaking period ? Two or more

stations may try to send RTS frames at the same time. These control frames may collide.

- If a collision occurs with an RTS or CTS MPDU, for less bandwidth is wasted in comparison to a large data MPDU. However, for a lightly loaded medium the overhead of the RTS/CTS frame transmission imposes additional delay.
- Wireless channels cannot handle very long transmissions due to their relatively large error rates.

2.2.3.4 Fragmentation

- Large MSDUs handed down from the LLC to the medium access control may require fragmentation to increase transmission reliability.
- To determine whether to perform fragmentation, MDPUs are compared to the manageable parameters, Fragmentation_Threshold. If the MPDU size exceeds the value of Fragmentation_Threshold, then the MSDU is broken into multiple fragments.

2.2.4 Frame Format

- Fig. 2.2.6 shows the frame format for IEEE 802.11. The MAC layer frame consists of nine fields.

2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0 to 2312 bytes	4 bytes
FC	D	Address 1	Address 2	Address 3	SC	Address 4	Frame body	FCS

Frame control										
Protocol version	Type	Subtype	To DS	From DS	More flag	Retry	Pwr mgt	More data	WEP	Rsvd
2 bits	2 bits	4 bits	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit

Fig. 2.2.6 Frame format

1. Frame Control (FC) : This field is 2 bytes long and define the type of frame and some control information.

Subfields of frame control

Field	Explanation
Version	The current version is 0.
Type	Type of information : management (00), control (01) or data (10).

Subtype	Defines the subtype of each type.
To DS	Defined later.
From DS	Defined later.
More flag	When set to 1, means more fragments.
Retry	When set to 1, means retransmitted frame.
Pwr mgt	When set to 1, means station is in power managment mode.
More data	When set to 1, means station has more to send.
WEP	Wired equivalent privacy. When set to 1, means encryption implemented.
Rsvd	Reserved.

2. **D :** In all frame types except one, this field defines the duration of the transmission that is used to set the value of NAV. In one control frame, this field defines the ID of the frame.
3. **Addresses :** There are four address fields, each 6 bytes long. The meaning of each address field depends on the value of the **To DS** and **From DS** sub fields.
4. **Sequence control :** This field defines the sequence number of the frame to be used in flow control.
5. **Frame body :** Frame body is in between 0 and 2312 bytes, contains information based on the type and subtype defined in the FC field.
6. **FCS :** The FCS field is 4 bytes long and contains a CRC-32 error detection sequence.

Frame Types

802.11 LAN defines three types of frames

1. Management frames 2. Control frames. 3. Data frames.

Management frames : Initial communication between stations and access points, the management frames are used.

Control frames : Control frames are used for accessing the channel and acknowledging frames. Fig. 2.2.7 shows the control frames.

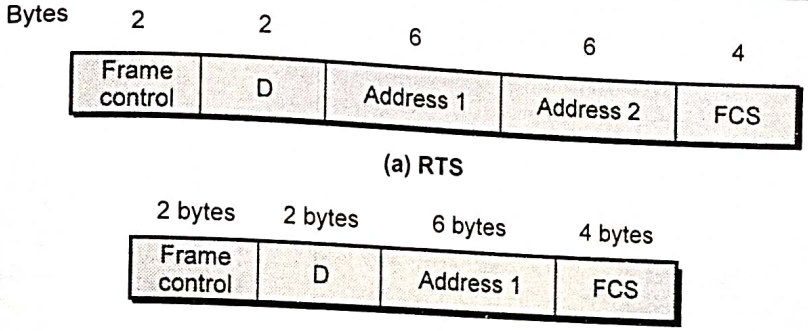


Fig. 2.2.7 Control frames

Values of subfields in control frames.

Subtype	Meaning
1011	Request to send
1100	Clear to send
1101	Acknowledgement

Data frames : Data frames are used for carrying data and control information.

2.2.5 Addressing Mechanism

- The IEEE 802.11 addressing mechanism specifies four cases, defined by the value of the two flags in the FC field, **To DS** and **From DS**. Following table shows all the conditions.

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

- Fig. 2.2.9 shows the FHSS physical layer.

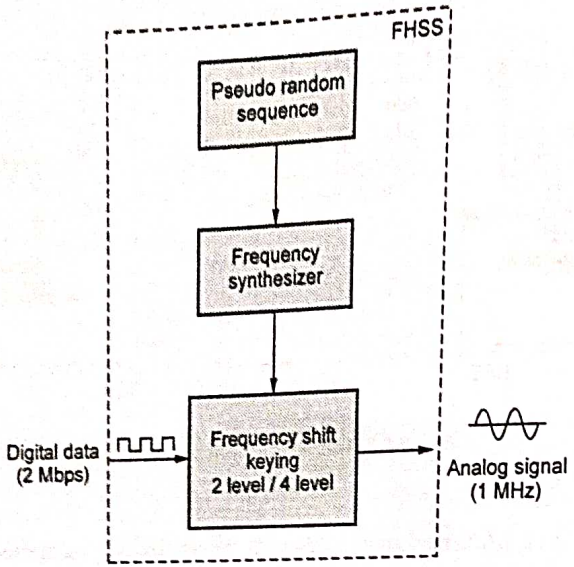


Fig. 2.2.9 FHSS

IEEE 802.11 DSSS

- It uses the direct sequence spread spectrum method. Fig. 2.2.10 shows the physical layer of DSSS.

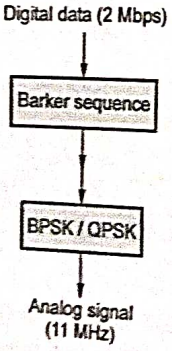


Fig. 2.2.10 DSSS

- DSSS uses the 2.4 GHz ISM band. The modulation technique is this specification is PSK at 1 Mbaud/s.
- The system allows 1 or 2 bits/baud which result in a data rate of 1 or 2 Mbps.

IEEE 802.11 Infrared

- It uses infrared light in the range of 800 to 900 nm. The modulation technique is called Pulse Position Modulation (PPM).
- Fig. 2.2.11 shows the physical layer of Infrared.

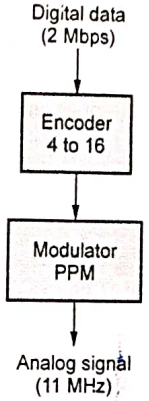


Fig. 2.2.11 Infrared

- For a 1-Mbps data rate, a 4-bit sequence is first mapped into a 16-bit sequence in which only one bit is set to 1 and rest to set to 0.

IEEE 802.11a OFDM

- It describes the orthogonal frequency division multiplexing method for signal generation in a 5-GHz ISM band.
- OFDM uses PSK and QAM for modulation. The common data rates are 18 Mbps for PSK and 54 Mbps for QAM.

2.2.7 CSMA/CA

- Wireless networks cannot use CSMA/CD in the MAC sublayer, since this requires the ability to receive and transmit at the same time - hence the use of CSMA/CA.
- In a wireless network, much of the sent energy is lost in transmission. The received signal has very little energy. Therefore, a collision may add only 5 to 10 percent additional energy. This is not useful for effective collision detection. We need to avoid collision on wireless networks because they cannot be detected. So CSMA/CA was invented for this network.
- Collisions are avoided by using three methods.
  a. Inter-frame space b. Contention window
  c. Acknowledgments.

- Fig. 2.2.12 shows the all three method of CSMA/CA.

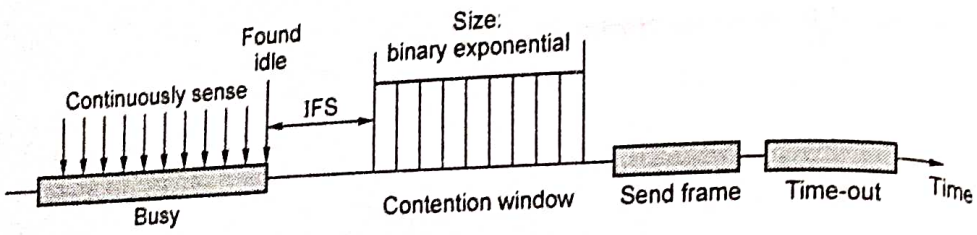


Fig. 2.2.12 CSMA/CA methods

Inter-frame space

- Collisions are avoided by deferring transmission even if the channel is found idle.
- When an idle channel is found, the station does not send immediately. It waits for a period of time called the Inter-Frame Space (IFS).
- In CSMA/CA, the IFS can also be used to define the priority of a station of a frame. A station that is assigned shorter IFS has a higher priority.

Contention window

- Contention windows are an amount of time divided into slots. A station that is ready to send chooses a random number of slots as its wait time.
- Station set one slot for the first time and then double each time the station cannot detect an idle channel after the IFS time.
- In this method, the station needs to sense the channel after each time slot
- If the station finds the channel busy, it does not restart the process; it just stops the timer and restarts it when the channel is sensed as idle.
- This method gives the priority to the station with the longest waiting time.

Acknowledgments

- The data may be corrupted during the transmission. The positive acknowledgment and the time out can help guarantee that the receiver has received the frame.
- Fig. 2.2.13 shows the flowchart for CSMA/CA.
(Refer Fig. 2.2.13 on next page).

2.2.4 Hidden Node Problem

- In the case of wireless network it is possible that A is sending a message to B, but C is out of its range and hence while "listening" on the network it will find the network to be free and might try to send packets to B at the same time as A. So, there will be a collision at B.

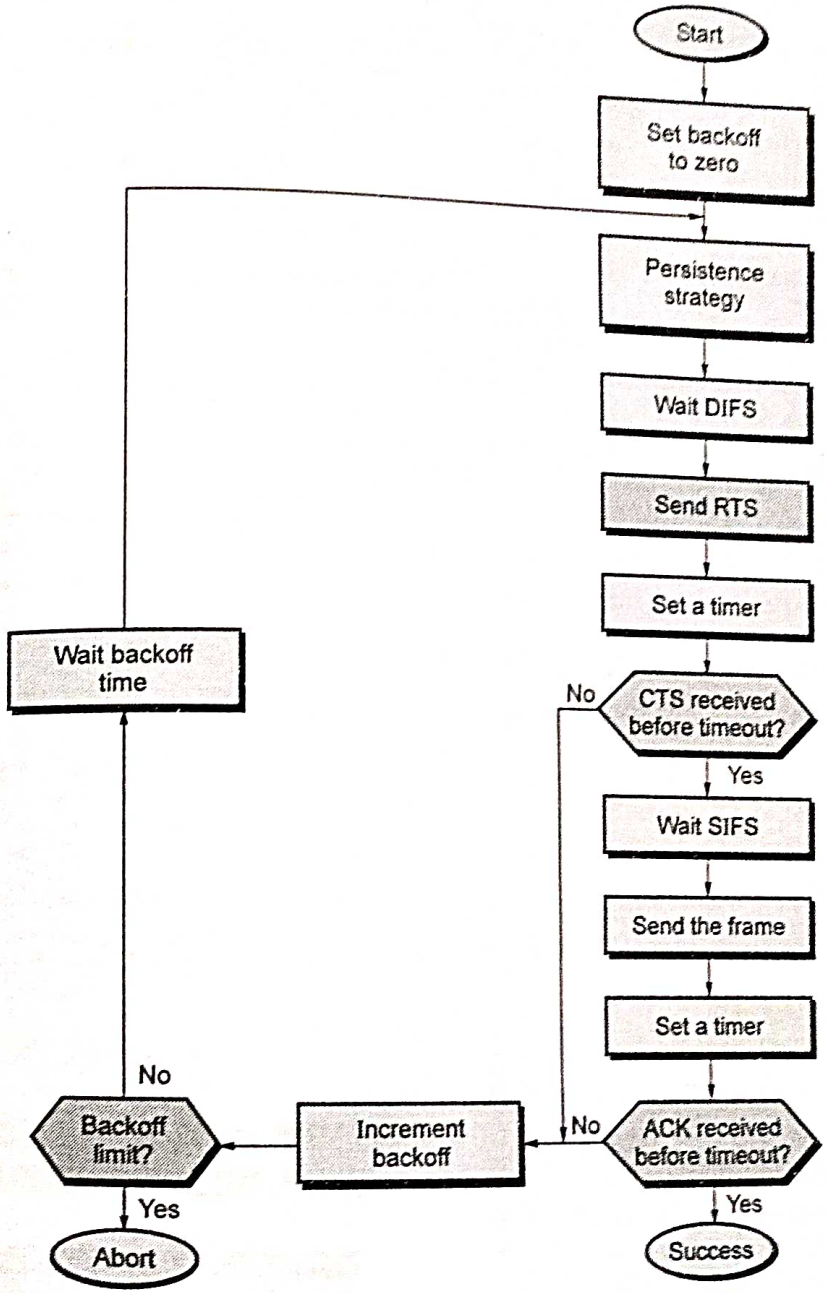


Fig. 2.2.13 Flowchart for CSMA/CA

- The problem can be looked upon as if A and C are hidden from each other. Hence it is called the "hidden node problem".
- Fig. 2.2.14 shows node A is transmitting.

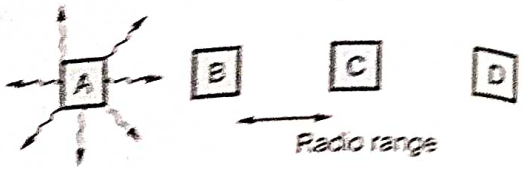


Fig. 2.2.14 A transmitting

2.2.2 Exposed Node Problem

- If C is transmitting a message to D and B wants to transmit a message to A, B will find the network to be busy as B hears C transmitting. Even if B would have transmitted to A, it would not have been a problem at A or D.
- CSMA/CD would not allow it to transmit message to A, while the two transmissions could have gone in parallel
- Fig. 2.2.15 shows node B is transmitting.

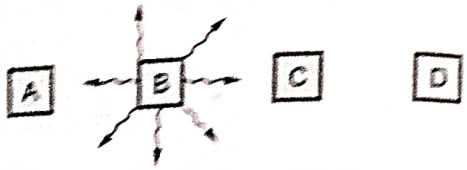


Fig. 2.2.15 B transmitting

2.2.3 Difference between 802.11a and 802.11b

Parameters	802.11a	802.11b
Raw data rates	Up to 54 Mbps (54, 48, 36, 24,18, 12 and 6 Mbps)	Up to 11 Mbps (11, 5.5, 2 and 1 Mbps)
Range	50 Meters	100 Meters
Bandwidth	UNII and ISM (5 GHz range)	ISM (2.4000-2.4835 GHz range)
Modulation	OFDM technology	DSSS technology

Review Questions

1. Describe MAC layer mechanism of IEEE 802.11.
   SPPU : Dec.-14, May-16, (End Sem.), Marks 10
2. Explain architecture of 802.11.
   SPPU : May-15, (End Sem.), Marks 10
3. What are different technical issues to implement WLAN ?
   SPPU : May-15, (End Sem.), Marks 8
4. Explain IEEE 802.11 FHSS and DSSS.
   SPPU : Dec.-15, (End Sem.), Marks 8

5. Explain the basic architecture of WLAN and discuss various components in it.
   SPPU : Dec.-15, May-17, (End Sem.), Marks 8
6. Describe with neat diagram WLAN architecture.
   SPPU : May-16 (End Sem.), Marks 8
7. What are hidden station and exposed station problems in WLAN ?
   SPPU : Dec.-16 (End Sem.), Marks 8
8. Explain BSS and ESS in 802.11.
   SPPU : Dec.-16 (End Sem.), Marks 8

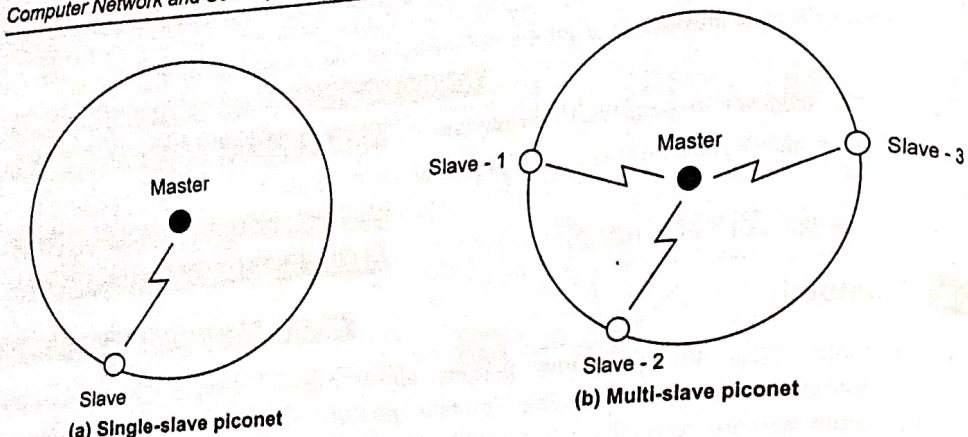
2.3 Bluetooth

SPPU : Dec.-14,16, May-15,16,17

- Bluetooth is a low-cost, low power, short range wireless communication technology used in networking, mobile phones and other portable device. Bluetooth wireless technology also enables devices to communicate with each other as soon as they come within range; no need to connect, plug into, install, enable or configure anything. Although the range of each Bluetooth device is approximately 10 meters but this distance can be increased to 100 meters with optional amplifiers placed at strategic locations within a building. Bluetooth does not need to be set-up it is always on. The device to communicate do not even require line-of-sight communication.
- Different devices can be automatically link-up with each other as soon as they come into range i.e. it creates a temporary network or **Personal Area Network (PAN)**. The Bluetooth specification is an open global specification defining the complete system upto application level. The Bluetooth promotors group has made Bluetooth an open specification, rather than keeping it restricted and proprietary, because more consumers can adopt it as many manufacturers are producing it.
- Bluetooth technology uses the globally available unlicensed ISM radio band of 2.4 GHz. The ISM (Industrial, Scientific and Medical) band frequency 2.4 - 2.484 GHz do not require an operator's license. From any authority, Bluetooth supports both voice and data as it supports both circuit switching and packet switching.

2.3.1 Bluetooth Architecture

- The basic element of a Bluetooth is **piconet**.
  Piconet is a collection of slave devices operating together with one common master as shown in Fig. 2.3.1. The Fig. 2.3.1 shows both single and multi slave piconet.
- As shown in Fig. 2.3.1 there is no direct link between slaves. A common master is shared between maximum seven slaves. (See Fig. 2.3.1 on next page)



(a) Single-slave piconet (b) Multi-slave piconet

Fig. 2.3.1 Piconet types

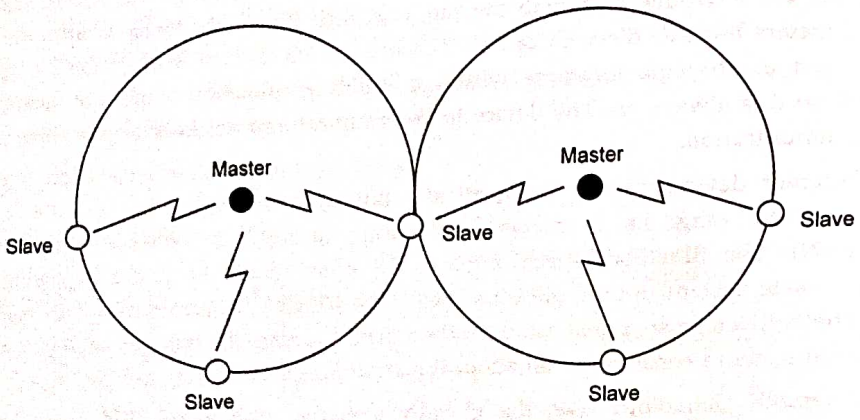


Fig. 2.3.2 Scatternet

- Several piconets can be established and linked together in a topology called a **scatternet**. In scatternet some devices are common to more than one piconet as shown in Fig. 2.3.2.
- Only one piconet can be active at any time. Different piconets in a scatternet can participate through Time Division Multiplexing (TDM) sharing a common channel.

2.3.2 Radio Layer

- Radio layer is roughly equivalent to the physical layer of the Internet model. Fig. 2.3.3 shows the bluetooth layers.
- Bluetooth devices are low-power and have a range of 10 m.

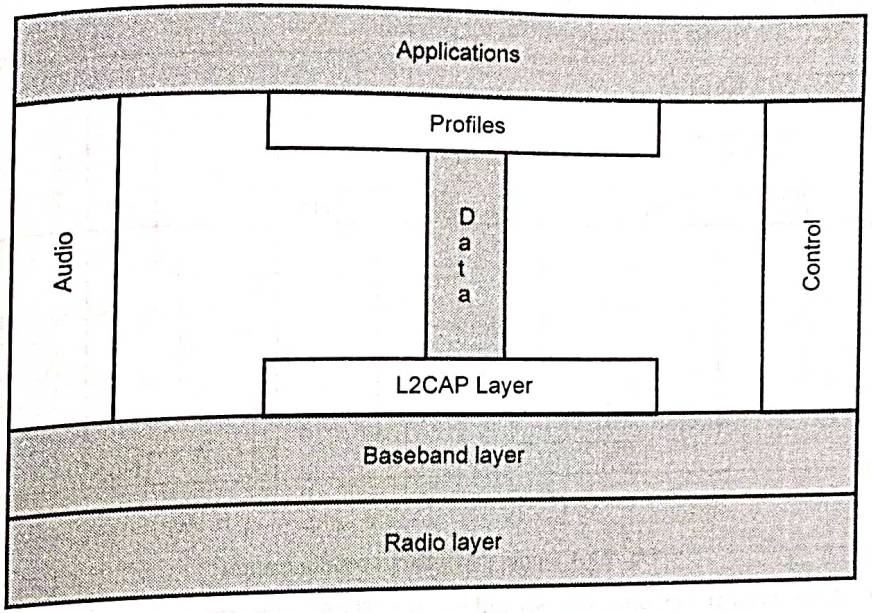


Fig. 2.3.3 Bluetooth layers

- **Band :** Bluetooth uses a 2.4 GHz ISM band divided into 79 channels of 1 MHz each.
- **FHSS :** Bluetooth uses frequency hopping spread spectrum method in the physical layer to avoid interference from other devices or other networks. Bluetooth hops 1600 times per second. A device uses a frequency for only 625 microseconds before it hops to another frequency.
- **Modulation :** To transfer bits over a signal, Bluetooth uses a sophisticated version of FSK, called GFSK. GFSK has a carrier frequency.

2.3.3 Baseband Layer

- This layer is equivalent to MAC sublayer in LAN. The access method is TDMA. The primary (master) and secondary (slave) communicate with each other using time slots.
- The length of the time slot is exactly the same as the dwell time, 625 microseconds.
- **TDMA :** Bluetooth uses a form of TDMA that is called time division duplex TDMA (TDD-TDMA). TDD-TDMA uses half-duplex communication.

Single Secondary Communication

- Fig. 2.3.4 shows the single secondary communication.

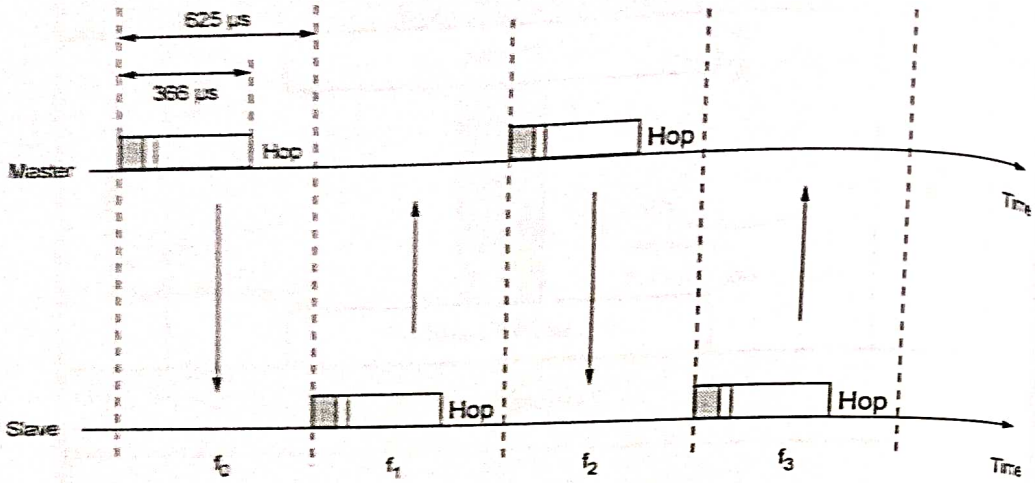


Fig. 2.3.4 Single secondary communication

- If the piconet has only one secondary, the TDMA operation is very simple. The time is divided into slots of 625 microseconds.
- The primary uses even-numbered slots and secondary uses odd-numbered slots. TDD-TDMA is half-duplex.
- In slot 0, the primary sends, the secondary receives; in slot 1, the secondary send and the primary receives.

Multiple Secondary Communications

- The number of secondary (slave) is more than one. The primary (Master) uses even-numbered slots and secondary uses odd-numbered slots.
- All secondary listen on even numbered slots, but only one secondary sends in any odd numbered slot. Fig. 2.3.5 shows the multiple secondary communications method. (See Fig. 2.3.5 on next page)
- In slot 0, the master sends a frame to slave 1.
- In slot 1, only slave 1 sends a frame to the primary because the previous frame was addressed to secondary 1; otherwise slaves are silent.
- In slot 2, the master sends a frame to slave 2.
- In slot 3, only slave 2 sends a frame to the primary because the previous frame was addressed to slave 2; other slaves are silent.
- The cycle continues.

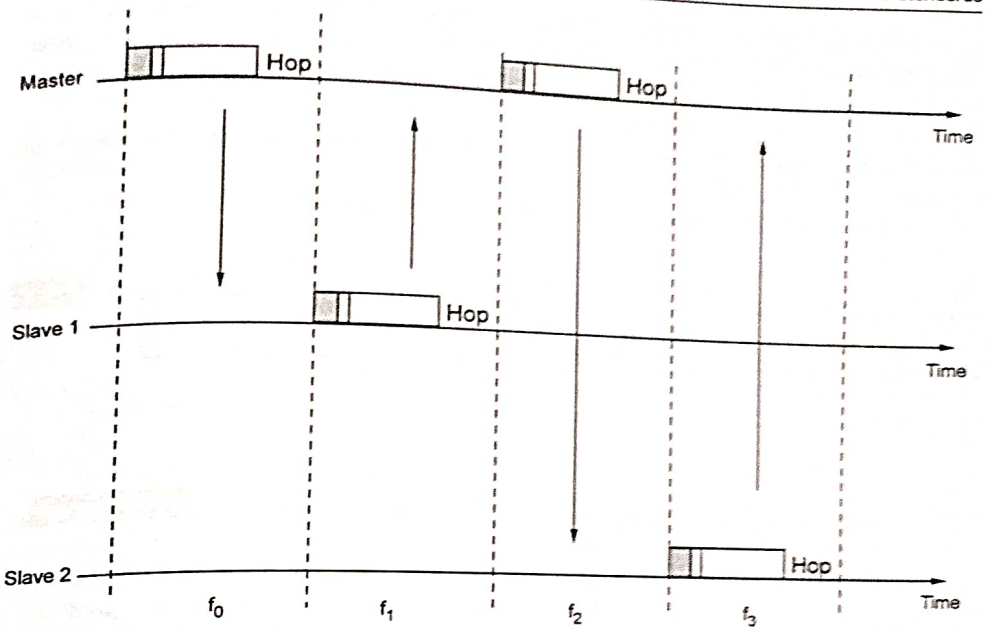


Fig. 2.3.5 Multiple secondary communications

Physical Links

- Two types of links are created between the master and slave : SCO links and ACL links.
- **Synchronous Connection Oriented** (SCO) link is used when avoiding latency is more important than integrity. SCO is used for real time audio where avoiding delay is all important.
- An **Asynchronous Connectionless Link** (ACL) is used when data integrity is more important than avoiding latency.

2.3.4 Frame Format

- A frame in the baseband layer can be one of three types :
  a. One-slot b. Three-slot c. Five-slot
- For one-slot frame exchange, 259 microseconds is needed for hopping and control mechanism. This means that a one slot frame can list only 625-259 or 366 microseconds.
- Three slot frames occupies three slots. However 259 microsecond is used for hopping, the length of the frame is $3 \times 625 - 259 = 1616$ microsecond or 1616 bits.

A device that uses a three slot frame remains at the same hop for three slot i.e. it uses same carrier frequency. Even through only one hop number is used, three hop numbers are consumed. That means the hop number for each frame is equal to the first slot of the frame.

- A five slot frame also uses 259 bits for hopping, which means that the length of the frame is
  $5 \times 625 - 259 = 2866$ bits. Fig. 2.3.6 shows the frame format.

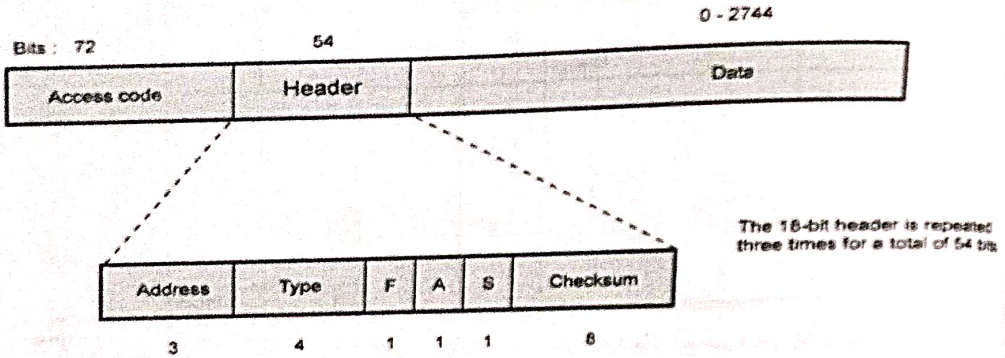


Fig. 2.3.6 Bluetooth data frame

- It begins with **access code** that usually identifies the master and slaves within radio range of two masters can tell which traffic is for them. Next field is a 54-bit **header** containing typical MAC sublayer fields. Then the **data field**, of up to 2744 bits (for a five-slot transmission). For a single time slot, the format is the same except that the data field is 240 bits.
- Header field consists of following,

1. **Address :** This field is identifies which of the eight active devices the frame is intended for. If the address is zero, it is used for broadcast communication from primary to all secondaries.
2. **Type :** This 4 bits field identifies the frame type (ACL, SCO, poll or null), the type of error correction used in the data field, and how many slots long the frame is.
3. **Flow (F) :** The flow subfield is 1-bit for flow control. When it is set to 1 then it is asserted by a slave when its buffer is full and cannot receive any more data.
4. **ACK (A) :** The 1-bit ack subfield is used to piggyback an ACK into a frame. Bluetooth uses stop and wait ARQ; 1-bit is sufficient for acknowledgement.
5. **Sequence (S) :** This 1-bit subfield is used to number the frames to detect retransmissions. The protocol is stop-and-wait, so 1 bit is enough.

6. **Checksum :** The 8-bit header error correction subfield is checksum to detect errors in each 18-bit header section. The 18-bit header is repeated three times for a total of 54 bits header. On the receiving side, a simple circuit examines all three copies of each bit. If all three are the same, the bit is accepted. If not, the majority opinion wins. Thus, 54-bits of transmission capacity are used to send 10 bits of header. The reason is that to reliably send data in a noisy environment using cheap, low-powered (2.5 mW) devices with little computing capacity, a great deal of redundancy is needed.

2.3.5 L2CAP

- L2CAP is Logical Link Control and Adaptation Protocol. This provides segmentation and re-assembly services to allow large packets to pass across Bluetooth links, also provides multiplexing for higher layer protocol and services. The L2CAP layer has three major functions :

1. It accepts packets of upto 64 kB from the upper layers and breaks them into frames for transmission. At the far end, the frames are reassembled into packets again.
2. It handles the multiplexing and demultiplexing of multiple packets sources. When a packet has been reassembled, the L2CAP layer determines which upper-layer protocol to hand it to, for example, RF communication or telephony.
3. L2CAP handles the quality of service requirement, both when links are established and during normal operation. Also negotiating at setup time is the maximum payload size allowed, to prevent a large-packet device from droping a small-packet device. This future is needed because not all devices can handle the 64 kB maximum packet. This layer corresponds with 802 Data Link Layer, that usually is responsible for transmission, framing, and error control over a particular link and as such, overlaps the link controller task and the control end of the baseband, including error checking and correction.

- Fig. 2.3.7 shows the data packet frame.

Length	Channel ID	Data and Control
2 bytes	2 bytes	0 - 65535 bytes

Fig. 2.3.7 Data packet frame

1. **Length :** The 16 bits field defines the size of the data, in bytes, coming from the upper layers.
2. **Channel ID (CID) :** The 16 bits CID defines a unique identifier for the virtual channel created at this level.
3. **Data :** Data can be up to 65535 bytes.

- Fig. 2.3.8 shows the L2CAP's position in the Bluetooth protocol stack.

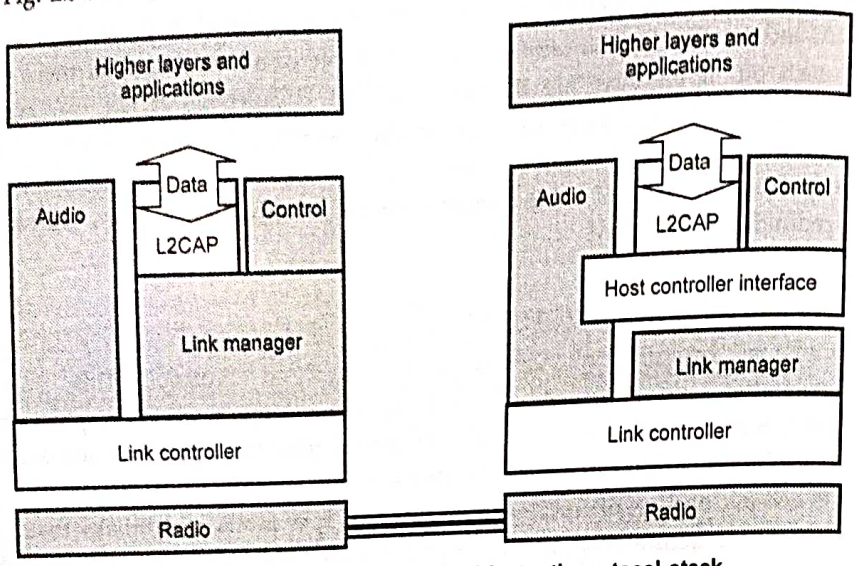


Fig. 2.3.8 L2CAP's position in the Bluetooth protocol stack

- Logical Link Control and Adaptation Protocol take data from higher layer of the Bluetooth stack and from applications and send it over the lower layers of the stack. L2CAP passes packet either to the Host Controller Interface (HCI) or in a host-less system, L2CAP passes packet directly to the Link Manager (LM). The Fig. 2.3.8 shows L2CAP's position in the Bluetooth stack for the cases with and without a HCI. Note that L2CAP transfers data, not audio.
- **L2CAP has many functions :**

a. **Multiplexing** between different higher layer protocols, allowing them to share lower layer links.

b. **Segmentation** and reassembly to allow transfer of larger packets than lower layers supports. L2CAP divides these large packets into segments and adds extra information to define the location of the segments in the original packet. The L2CAP segments the packet at the source and reassembles them at the destination.

c. **Group management**, providing one-way transmission to a group of other Bluetooth devices.

d. **Quality of service management** for higher protocols.

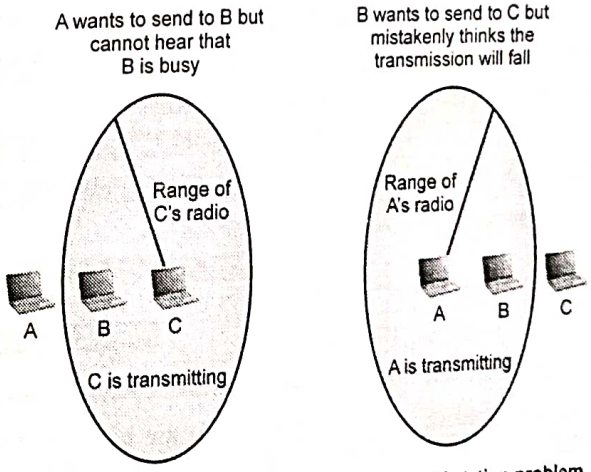
- L2CAP relies on ACL connections to pass data reliable from end to end. A separate control function must set up the ACL connections when they required by L2CAP, and close them down when they are no longer required. L2CAP also relies upon the ACL connection's quality of service to provide the quality of service negotiated with higher layers.

2.3.6 Hidden Station Problem

Hidden station problem : The 802.11 MAC sublayer protocol is quite different from that of Ethernet due to the inherent complexity of the wireless environment compared to that of a wired system. With Ethernet, a station just waits until the ether goes silent and starts transmitting. If it does not receive a noise burst back within the first 64 bytes, the frame has almost assuredly been delivered correctly. With wireless, this situation does not hold.

To start with, the hidden station problem in Fig. 2.3.9. Since not all stations are within radio range of each other, transmissions going on in one part of a cell may not be received elsewhere in the same cell. In this example, station C is transmitting to station B. If A senses the channel, it will not hear anything and falsely conclude that it may now start transmitting to B.

In addition, there is the inverse problem, the exposed station problem, illustrated in Fig. 2.3.9. Here B wants to send to C so it listens to the channel. When it hears a transmission, it falsely concludes that it may not send to C, even though A may be transmitting to D (not shown). In addition, most radios are half duplex, meaning that they cannot transmit and listen for noise for noise bursts at the same time on a single frequency. As a result of these problems, 802.11 does not use CSMA/CD, as Ethernet does.



(a) Hidden station problem **(b) The exposed station problem**

Fig. 2.3.9

2.3.7 Comparison between IEEE 802.11x and Bluetooth

Sr. No.	Parameter	IEEE 802.11	Bluetooth
1.	HOP frequency	2.5 Hops/sec	1600 Hops/sec.
2.	Data transfer rate	11 Mbps	1 Mbps
3.	Modulation techniques	Complementary Code Keying (CCK)	Gaussian Frequency Shift Keying (GFSK)
4.	Transmission power	More power required	Less power required
5.	Transmission range (Distance)	15 to 150 meters for indoors and 300 meters for outdoors	10 meters
6.	Application	a) For LAN b) For Larger time network	a) For short time N/W b) For close proximity

Review Questions

1. Describe bluetooth protocol stack. **SPPU : May-15, Dec.-16, (End Sem.), Marks 10**
2. Explain in detail architecture of bluetooth. **SPPU : Dec.-14, May-15, (End Sem.), Marks 10**
3. Explain bluetooth architecture. **SPPU : May-16, (End Sem.), Marks 8**
4. Compare bluetooth and 802.11. What are the limitations of bluetooth. **SPPU : Dec-16, (End Sem.), Marks 8**
5. Compare : Bluetooth and wireless LAN. **SPPU : May-17, (End Sem.), Marks 8**
6. Explain bluetooth features and architecture with suitable diagram. **SPPU : May-17, (End Sem.), Marks 10**

2.4 IEEE 802.16

SPPU : Dec.-14, May-16,17

- WiMAX stands for Worldwide Interoperability for Microwave Access.
- WiMAX refers to broadband wireless networks that are based on the IEEE 802.16 standard, which ensures compatibility and interoperability between broadband wireless access equipment.
- WiMAX, which will have a range of upto 31 miles, is primarily aimed at making broadband network access widely available without the expense of stringing wires or the distance limitations of digital subscriber line.

- WiMAX uses Orthogonal Frequency Division Multiplexing (OFDM) and connectivity at speeds upto 70 Mbps.
- WiMAX is a wireless WAN technology. A WIMAX system consists of

1. **A WiMAX tower,** similar in concept to a cell-phone tower - A single WiMAX tower can provide coverage to a very large area as big as 3000 square miles (~8000 square km).
2. **A WiMAX receiver** : The receiver and antenna could be a small box or Personal Computer Memory card or they could be built into a laptop the way WiFi access is today.

2.4.1 802.16 Protocol Stack

- Fig. 2.4.1 shows the 802.16 protocol stack. The bottom sublayer deals with transmission. Traditional narrowband radio is used with conventional modulation schemes. Transmission convergence sublayer hide the different technologies from the data link layer.

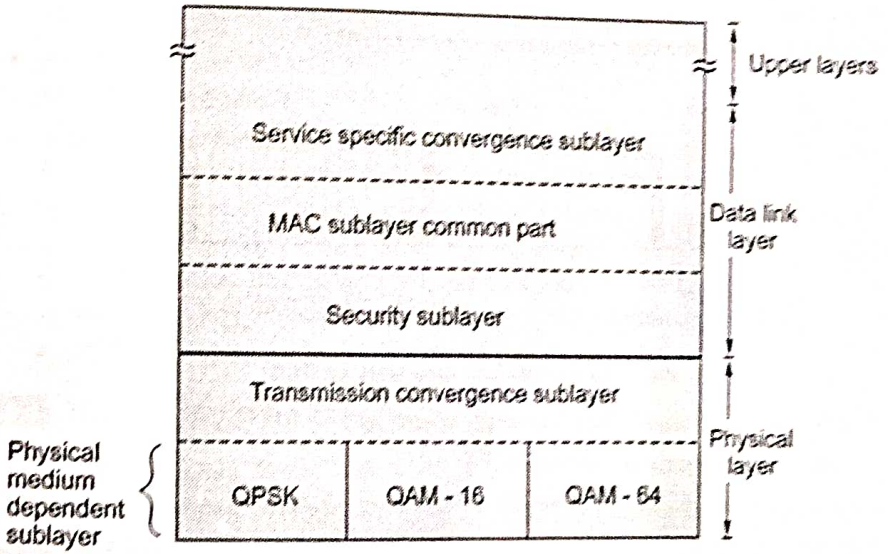


Fig. 2.4.1 802.16 protocol stack

- The **802.16a** standard will support OFDM in the **2-to-11 GHz** frequency range. The **802.16b** standard will operate in the **5 GHz ISM band.**
- The data link layer consists of three sublayers. **Security sublayer** deals with privacy and security. It manages encryption, decryption and key management. The

MAC sublayer common part is responsible for channel management. It can schedule the downstream channels very efficiently and plays a major role in managing the upstream channels as well. It is completely connection-oriented, in order to provide quality-of-service guarantee for telephony and multimedia communication.

- Service specific convergence sublayer's function is to interface to the network layer. The 802.16 was designed to integrate seamlessly with both datagram protocols (e.g. PPP, IP and Ethernet) and ATM. The problem is that packet protocols are connectionless and ATM is connection oriented.

2.4.2 The 802.16 Physical Layer

- 802.16 employs three different modulation schemes, depending on how far the subscriber station is from the base station.

1. For close-in subscriber, QAM-64 is used, with 6 bits/baud.
2. For medium-distance subscribers, QAM-16 is used, with 4 bits/baud.
3. For distant subscribers, QPSK is used, with 2 bits/baud.

- Fig. 2.4.2 shows the frames and time slots for TDD.

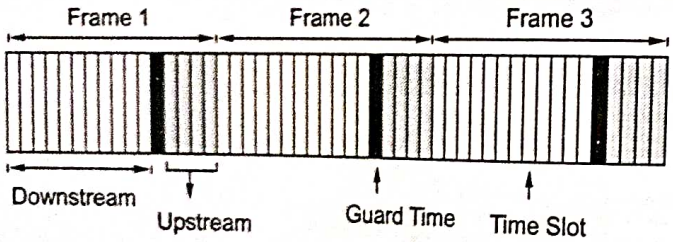


Fig. 2.4.2 Frames and time slots for TDD

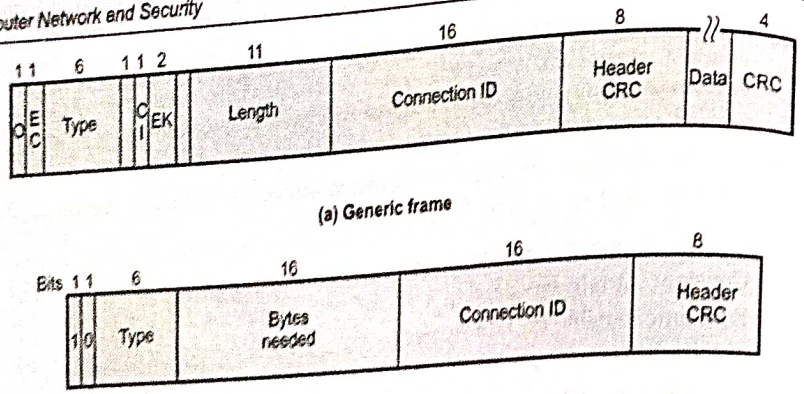
- 802.16 uses two schemes for bandwidth allocation.
  1. Frequency Division Duplexing (FDD)
  2. Time Division Duplexing (TDD).
- Downstream traffic is mapped onto time slots by the base station. The base station is completely in control for this direction. Upstream traffic is more complex and depends on the quality of service required.
- Hamming code is used to do forward error correction in the physical layer.

2.4.3 The 802.16 MAC Sublayer Protocol

- MAC frames occupy an integral number of physical layer time slots. Each frame is composed of subframes, the first two of which are the downstream and upstream maps. The downstream map also contains various system parameters to inform new station as they come on-line.
- Upstream channel define four classes of services,
  1. Constant bit rate service.
  2. Real-time variable bit rate service.
  3. Non-real-time variable bit rate service.
  4. Best-effort service.
- All service in 802.16 is connection oriented.
- Constant bit rate service is intended for transmitting uncompressed voice such as on a T1 channel.
- Real-time variable bit rate service is for compressed multimedia and other soft real-time applications in which the amount of bandwidth needed each instant may vary.
- Non-real-time variable bit rate service is for heavy transmissions that are not real time, such as large file transfers.
- Finally, best-effort service is for everything else. No polling is done and the subscriber must contend for bandwidth with other best-efforts subscribers. Requests for bandwidth are done in time slots marked in the upstream map as available for contention. If a request is successful, its success will be noted in the next downstream map. If it is not successful, unsuccessful subscribers have to try again later. To minimize collisions the Ethernet binary exponential backoff algorithm is used.

2.4.4 The 802.16 Frame Structure

- All MAC frames begin with a generic header. The header is followed by an optional payload and an optional checksum (CRC). Fig. 2.4.3 shows frame structure. (See Fig. 2.4.3 on next page)
- The payload is not needed in control frames, for example, those requesting channel slots. The checksum is also optional due to the error correction in the physical layer.
  1. The **EC bit** tells whether the payload is encrypted.
  2. The **Type field** identifies the frame type, mostly telling whether packing and fragmentation are present.



(a) Generic frame

(b) Bandwidth request frame

Fig. 2.4.3 Frame structure

3. The **CI field** indicates the presence or absence of the final checksum.
4. The **EK field** tells which of the encryption keys is being used.
5. The **Length field** gives the complete length of the frame, including the header.
6. The **connection identifier** tells which connection this frame belongs to.
7. The **header CRC** field is a checksum over the header only, using the polynomial x^8+x^2+x+1.

2.4.5 Comparison between Wi-FI and WiMax

Parameters	Wi-FI	WiMax
IEEE standard	802.11	802.16
Typical link length	100 m	10 km
Typical bandwidth	54 Mbps (shared)	70 Mbps (shared)
Typical use	Link a notebook computer to a wired base	Link a building to a wired tower
Wired technology analogy	Ethernet	Co-axial cable

2.4.6 Wired Vs Wireless Networking

- The biggest difference between these two types of networks is one uses network cables and one uses radio frequencies.
- A wired network allows for a faster and more secure connection and can only be used for distances shorter than 2000 feet. A wireless network is a lot less secure and transmission speeds can suffer from outside interference.

- Although wireless networking is a lot more mobile than wired networking the range of the network is usually 150-300 indoors and upto 1000 feet outdoors depending on the terrain.
- The cost for wired networking has become rather inexpensive. Ethernet cables, hubs and switches are very inexpensive. Some connection sharing software packages, like ICS, are free; some cost a nominal fee. Broadband routers cost more, but these are optional components of a wired network and their higher cost is offset by the benefit of easier installation and built-in security features.
- Wireless gear costs somewhat more than the equivalent wired ethernet products. At full retail prices, wireless adapters and access points may cost three or four times as much as ethernet cable adapters and hubs/switches, respectively.
- Wired LANs offer superior performance. A traditional ethernet connection offers only 10 Mbps bandwidth, but 100 Mbps fast ethernet technology costs a little more and is readily available. Fast ethernet should be sufficient for file sharing, gaming and high-speed internet access for many years into the future. Wireless networks using 802.11b support a maximum bandwidth of 11 Mbps, roughly the same as that of old, traditional ethernet. 802.11a and 802.11g LANs support 54 Mbps, that is approximately one-half the bandwidth of fast ethernet. Furthermore, wireless networking performance is distance sensitive, meaning that maximum performance will degrade on computers farther away from the access point or other communication endpoint.
- In theory, wireless LANs are less secure than wired LANs, because wireless communication signals travel through the air and can easily be intercepted. The weaknesses of wireless security are more theoretical than practical. Wireless networks protect their data through the Wired Equivalent Privacy (WEP) encryption standard that makes wireless communications reasonably as safe as wired ones.

Review Questions

1. *Explain frame format of 802.16.* **SPPU : Dec.-14, May-16,17, (End Sem.), Marks 8**

2.5 Short Answered Questions

Q.1 Define hidden node problem.

Ans. : In wireless networking, hidden node problem occurs when a node is visible from a wireless Access Point (AP), but not from other nodes communicating with that AP.

Q.2 List bluetooth standards.

Ans. :

Class	Power	Range
Class 3	1 MW (0 dBm)	10 M
Class 2	2.5 MN (4 dBm)	20 M
Class 1	100 MN (20 dBm)	100 M

Q.3 List typical bluetooth applications.

Ans. :

1) Adhoc networking
2) Remote synchronization
3) Auto synchronization
4) Three in one handset
5) Cable replacement.

Q.4 State the performance characteristics of a typical bluetooth device.

Ans. :

1) Operating frequency - 2.4 GHz
2) Transmission power - 1 mW
3) Data rate - 720 kbps
4) Range - 10 meters
5) No. of devices - 8
6) Connectivity - Spread spectrum.

2.6 Multiple Choice Questions

Q.1 The Access Point (AP) in a wireless LAN is _____.

a) device that allows wireless devices to connect to a wired network
b) wireless devices itself
c) both device that allows wireless devices to connect to a wired network and wireless devices itself
d) all the nodes in the network

Q.2 _____ event is not possible in wireless LAN ?

a) Collision detection
b) Acknowledgement of data frames
c) Multi-mode data transmission
d) Connection to wired networks

Q.3 IEEE 802.11 standard is for_____.

a) wireless LAN
b) bluetooth
c) Wi-Fi
d) Wi-MAX

Q.4 IEEE standard for bluetooth _____.

a) 802.15.1
b) 802.15.2
c) 802.15.3
d) 802.15.4

Q.5 Access point is _____.

a) an entity that provides access to the LLC layer
b) an entity that provides access to the MAC layer
c) an entity that provides access to the distribution system
d) an entity that provides access to the basic service set

Answer Keys for Multiple Choice Questions :

Q.1	a	Q.2	a	Q.3	a
Q.4	a	Q.5	c		

❑❑❑