USN										

Internal Assessment Test 3 – May 2018

Sub:	Data Communication					Sub Code:	15CS46	Branch:	CSE
Date:	23/05/2018	Duration:	90 min's	Max Marks:	50	Sem / Sec:	IV A ,B,C		OBE

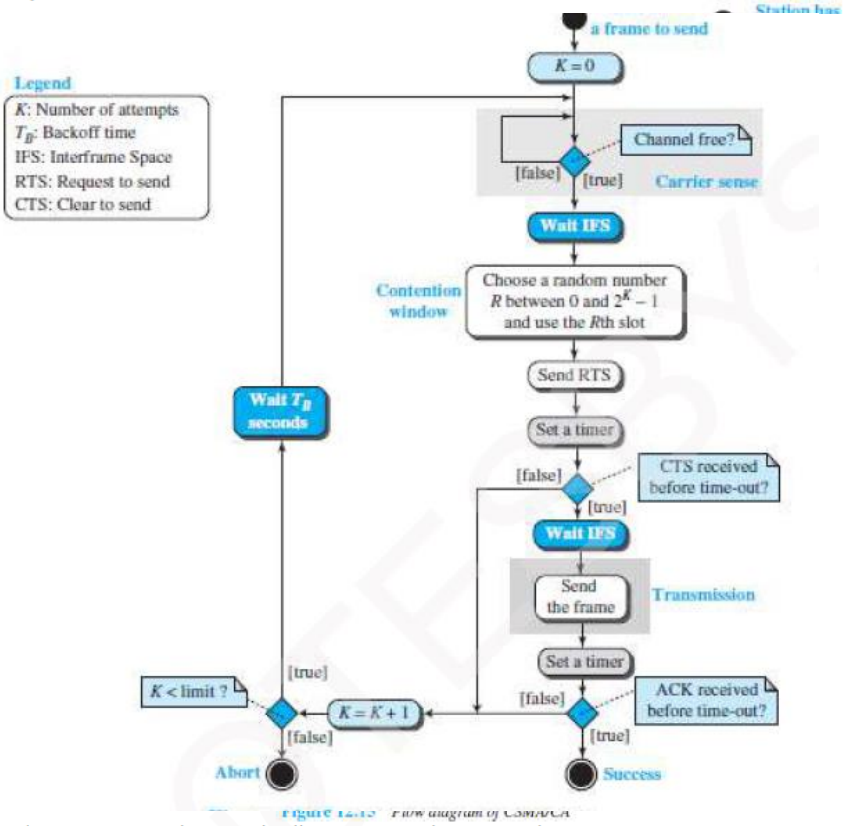
Answer any FIVE FULL Questions

		MARKS	CO	RBT
1	Explain the working of CSMA/CA Multiple Access protocol.	[10]	CO3	L2
2	Define Channelization. With an example, explain the working of CDMA channelization protocol.	[10]	CO3	L2
3	Explain the structure of IEEE 802.3 Ethernet frame format. Specify maximum and the minimum payload size supported by Ethernet frame.	[10]	CO3	L2
4 a.	Write a short note on Fast Ethernet.	[4]	CO3	L2
b.	Explain the different layers of Bluetooth Network.	[6]	CO4	L2
5 a.	With a neat diagram, explain the structure of IPV4 header format.	[06]	CO 5	L2
b.	List and explain the different extension headers used in IPV6.	[04]	CO 5	L2
6.	List and explain 3different categories of Satellites.	[10]	CO4	L2
7 a.	With a neat diagram, explain 3 phases the mobile host goes through to communicate with a remote station.	[06]	CO4	L2
b.	Write a note on 3G.	[04]	CO5	L2
8.	Explain the MAC 802.11 frame format.	[10]	CO4	L2

1. Explain the working of CSMA/CA Multiple Access protocol. [10]

4.2.4 CSMA/CA

- Here is how it works (Figure 12.15):
  1) A station needs to be able to receive while transmitting to detect a collision.
     i) When there is no collision, the station receives one signal: its own signal.
     ii) When there is a collision, the station receives 2 signals:
        a) Its own signal and
        b) Signal transmitted by a second station.
  2) To distinguish b/w these 2 cases, the received signals in these 2 cases must be different.



- CSMA/CA was invented to avoid collisions on wireless networks.
- Three methods to avoid collisions (Figure 12.16):
  1) Interframe space 2) Contention window and 3) Acknowledgments

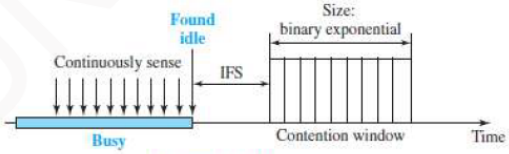


Figure 12.16 *Contention window*

1) Interframe Space (IFS)

- Collisions are avoided by deferring transmission even if the channel is found idle.
- When the channel is idle, the station does not send immediately.
  Rather, the station waits for a period of time called the inter-frame space or IFS.
- After the IFS time,
  if the channel is still idle,
  then, the station waits for the contention-time &
  finally, the station sends the frame.
- IFS variable can also be used to prioritize stations or frame types.
  For example, a station that is assigned a shorter IFS has a higher priority.

2) Contention Window

- The contention-window is an amount of time divided into time-slots.
- A ready-station chooses a random-number of slots as its wait time.
- In the window, the number of slots changes according to the binary exponential back-off strategy.
- For example:

  At first time, number of slots is set to one slot and
  Then, number of slots is doubled each time if the station cannot detect an idle channel.

3) Acknowledgment

- There may be a collision resulting in destroyed-data.
- In addition, the data may be corrupted during the transmission.
- To help guarantee that the receiver has received the frame, we can use

  i) Positive acknowledgment and
  ii) Time-out timer

4.2.4.1 Frame Exchange Time Line

- Two control frames are used:

  1) Request to send (RTS)
  2) Clear to send (CTS)
- The procedure for exchange of data and control frames in time (Figure 12.17):

  1) The source senses the medium by checking the energy level at the carrier frequency.
  ii) If the medium is idle,
  then the source waits for a period of time called the DCF interframe space (DIFS);
  finally, the source sends a RTS.

2) The destination
→ receives the RTS
→ waits a period of time called the short interframe space (SIFS)
→ sends a control frame CTS to the source.
CTS indicates that the destination station is ready to receive data.

3) The source
→ receives the CTS
→ waits a period of time SIFS
→ sends a data to the destination

4) The destination
→ receives the data
→ waits a period of time SIFS
→ sends a acknowledgment ACK to the source.
ACK indicates that the destination has been received the frame.

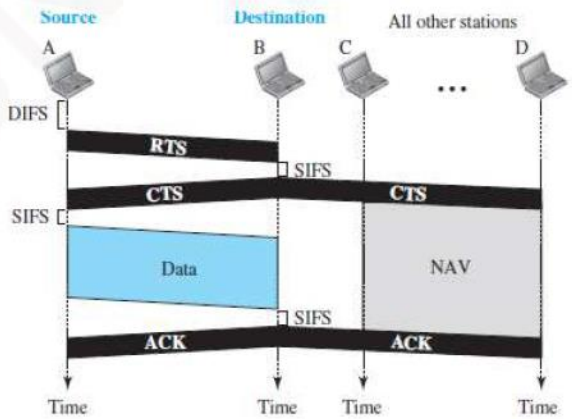


Figure 12.17 *CSMA/CA and NAV*

4.2.4.2 Network Allocation Vector

- When a source-station sends an RTS, it includes the duration of time that it needs to occupy the channel.
- The remaining stations create a timer called a network allocation vector (NAV).
- NAV indicates waiting time to check the channel for idleness.
- Each time a station accesses the system and sends an RTS frame, other stations start their NAV.

4.2.4.3 Collision during Handshaking

- Two or more stations may try to send RTS at the same time.
- These RTS may collide.
- The source assumes there has been a collision if it has not received CTS from the destination.
- The backoff strategy is employed, and the source tries again.

4.2.4.4 Hidden Station Problem

- Figure 12.17 also shows that the RTS from B reaches A, but not C.
- However, because both B and C are within the range of A, the CTS reaches C.
- Station C knows that some hidden station is using the channel and refrains from transmitting until that duration is over.

4.2.4.5 CSMA/CA and Wireless Networks

- CSMA/CA was mostly intended for use in wireless networks.
- However, it is not sophisticated enough to handle some particular issues related to wireless networks, such as hidden terminals or exposed terminals.

2 Define Channelization. With an example, explain the working of CDMA channelization protocol.[10]

The term channelization refers to the sharing of a point-to-point communications medium.1 For example, many telephone conversations (or in our context, computer-to-computer network transactions) can be submitted simultaneously on a single wire, with each conversation being on a separate channel.

4.4.3 CDMA

- CDMA simply means communication with different codes.
- CDMA differs from FDMA because
  → only one channel occupies the entire bandwidth of the link.
- CDMA differs from TDMA because
  → all stations can send data simultaneously; there is no timesharing.

(Analogy: CDMA simply means communication with different codes.
For example, in a large room with many people, 2 people can talk privately in English if nobody else understands English. Another 2 people can talk in Chinese if they are the only ones who understand Chinese, and so on).

4.4.3.1 Implementation

- Let us assume we have four stations 1, 2, 3, and 4 connected to the same channel.
- The data from station-1 are d_1, from station-2 are d_2, and so on.
- The code assigned to the first station is c_1, to the second is c_2, and so on.
- We assume that the assigned codes have 2 properties.
  1) If we multiply each code by another, we get 0.
  2) If we multiply each code by itself, we get 4 (the number of stations).

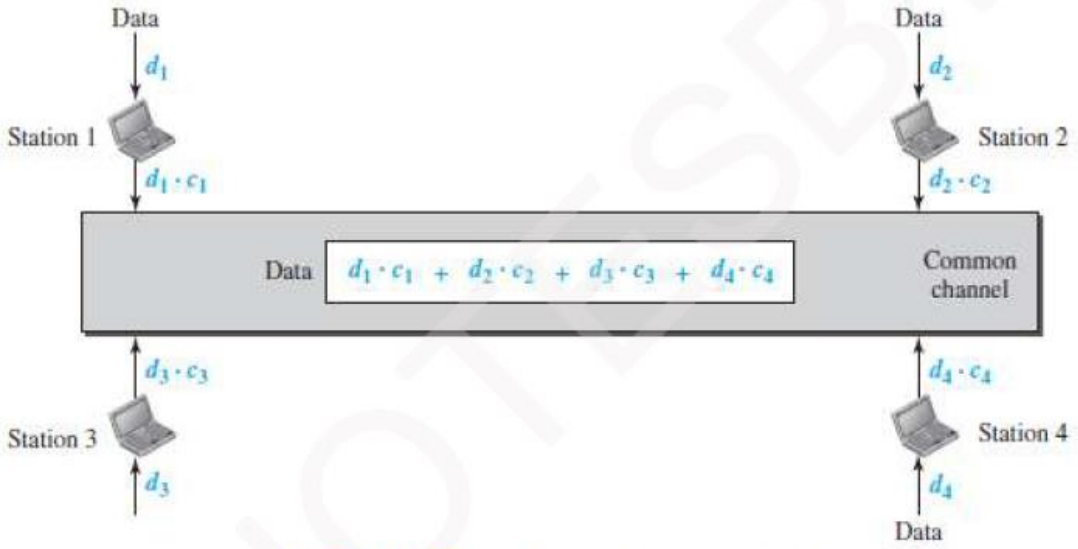


Figure 12.23 *Simple idea of communication with code*

- Here is how it works (Figure 12.23):
  - Station-1 multiplies the data by the code to get $d_1.c_1$.
  - Station-2 multiplies the data by the code to get $d_2.c_2$. And so on.
  - The data that go on the channel are the sum of all these terms.

$$d_1 \cdot c_1 + d_2 \cdot c_2 + d_3 \cdot c_3 + d_4 \cdot c_4$$

- The receiver multiplies the data on the channel by the code of the sender.
- For example, suppose stations 1 and 2 are talking to each other.
- Station-2 wants to hear what station-1 is saying.
- Station-2 multiplies the data on the channel by c_1 the code of station-1.

$(c_1.c_1)=4$, $(c_2.c_1)=0$, $(c_3.c_1)=0$, and $(c_4.c_1)=0$,

Therefore, station-2 divides the result by 4 to get the data from station-1.

$$\begin{aligned}\text{data} &= (d_1 \cdot c_1 + d_2 \cdot c_2 + d_3 \cdot c_3 + d_4 \cdot c_4) \cdot c_1 \\ &= d_1 \cdot c_1 \cdot c_1 + d_2 \cdot c_2 \cdot c_1 + d_3 \cdot c_3 \cdot c_1 + d_4 \cdot c_4 \cdot c_1 = 4 \times d_1\end{aligned}$$

4.4.3.3 Data Representation

- We follow the following rules for encoding:
  1) To send a 0 bit, a station encodes the bit as -1
  2) To send a 1 bit, a station encodes the bit as +1
  3) When a station is idle, it sends no signal, which is interpreted as a 0.

4.4.3.4 Encoding and Decoding

- We assume that
  - Stations 1 and 2 are sending a 0 bit.
  - Station-4 is sending a 1 bit.
  - Station-3 is silent.
- Here is how it works (Figure 12.26):
  - At the sender-site, the data are translated to -1, -1, 0, and +1.
  - Each station multiplies the corresponding number by its chip (its orthogonal sequence).
  - The result is a new sequence which is sent to the channel.
  - The sequence on the channel is the sum of all 4 sequences.
  - Now imagine station-3, which is silent, is listening to station-2.
  - Station-3 multiplies the total data on the channel by the code for station-2, which is [+1 -1 +1-1], to get

$$[-1\ -1\ -3\ +1] \cdot [+1\ -1\ +1\ -1] = -4/4 = -1 \rightarrow \text{bit 1}$$

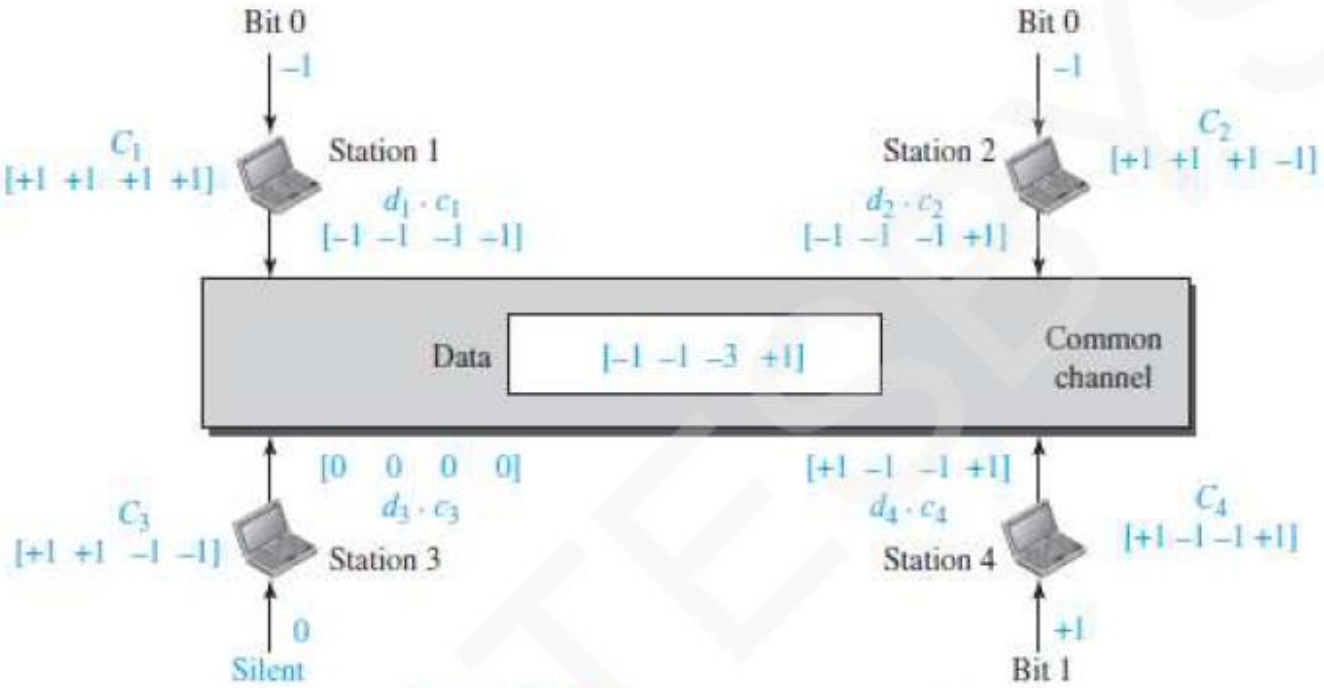


Figure 12.26 *Sharing channel in CDMA*

3 Explain the structure of IEEE 802.3 Ethernet frame format. Specify maximum and the minimum payload size supported by Ethernet frame. [10]

4.6.1.2 Frame Format

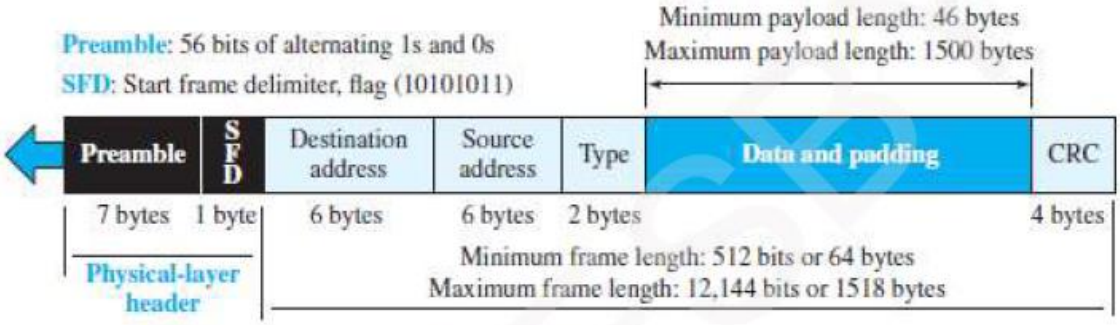


Figure 13.3 *Ethernet frame*

Figure 13.3 *Ethernet frame*

- The Ethernet frame contains 7 fields (Figure 13.3):

1) Preamble

- This field contains 7 bytes (56 bits) of alternating 0s and 1s.
- This field
  - → alerts the receiving-system to the coming frame and
  - → enables the receiving-system to synchronize its input timing.
- The preamble is actually added at the physical-layer and is not (formally) part of the frame.

2) Start Frame Delimiter (SFD)

- This field signals the beginning of the frame.
- The SFD warns the stations that this is the last chance for synchronization.
- This field contains the value: 10101011.
- The last 2 bits (11) alerts the receiver that the next field is the destination-address.

3) Destination Address (DA)

- This field contains the physical-address of the destination-station.

4) Source Address (SA)

- This field contains the physical-address of the sender-station.

5) Length or Type

- This field is defined as a i) type field or ii) length field.
  - i) In original Ethernet, this field is used as the type field.
    - ¤ Type field defines the upper-layer protocol using the MAC frame.
  - ii) In IEEE standard, this field is used as the length field.
    - ¤ Length field defines the number of bytes in the data-field.

¤ Length field defines the number of bytes in the data-field.

6) Data

- This field carries data encapsulated from the upper-layer protocols.
- Minimum data size = 46 bytes. Maximum data size = 1500 bytes.

7) CRC

- This field contains error detection information such as a CRC-32.

4.6.1.3 Frame Length

- Ethernet has imposed restrictions on both minimum & maximum lengths of a frame (Figure 13.5).

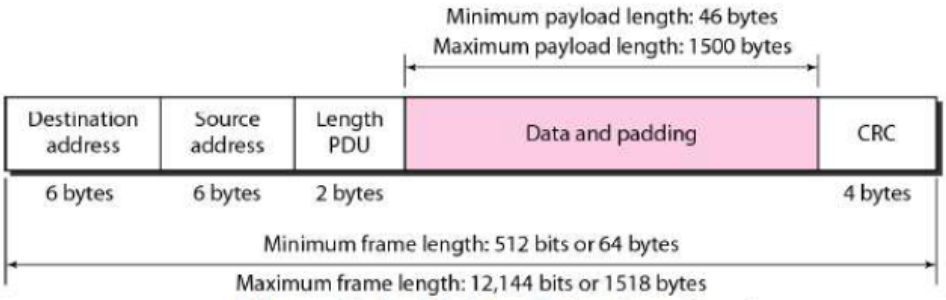


Figure 13.5 *Minimum and maximum lengths*

- The minimum length restriction is required for the correct operation of CSMA/CD.
- Minimum length of frame = 64 bytes.
  - 1) Minimum data size = 46 bytes.
  - 2) Header size + Trailer size = 14 + 4 = 18 bytes.

  (i.e. 18 bytes → 6 bytes source-address + 6 bytes dest-address + 2 bytes length + 4 bytes CRC).
- The minimum length of data from the upper layer = 46 bytes.
- If the upper-layer packet is less than 46 bytes, padding is added to make up the difference.
- Maximum length of frame =1518 bytes.
  - 1) Maximum data size = 1500 bytes.
  - 2) Header size + trailer size = 14 + 4 = 18 bytes.
- The maximum length restriction has 2 reasons:
  - 1) Memory was very expensive when Ethernet was designed.
    - A maximum length restriction helped to reduce the size of the buffer.
  - 2) This restriction prevents one station from
    - → monopolizing the shared medium
    - → blocking other stations that have data to send.

4 a. Write a short note on Fast Ethernet.

Fast-Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel.
Goals of Fast-Ethernet:
Upgrade the data-rate to 100 Mbps.
Make it compatible with Standard-Ethernet.
Keep the same 48-bit address.
Keep the same frame format.
Keep the same minimum and maximum frame-lengths.

Access Method

Access method is same in Standard-Ethernet.
Only the star topology is used.
For the star topology, there are 2 choices:
In the half-duplex approach, the stations are connected via a hub. CSMA/CD was used as access-method.
In the full-duplex approach, the connection is made via a switch with buffers at each port. There is no need for CSMA/CD.

Physical-layer

The physical-layer in Fast-Ethernet is more complicated than the one in Standard-Ethernet.
Some of the features of this layer are as follows. 1) Topology 2) Implementation and 3) Encoding.

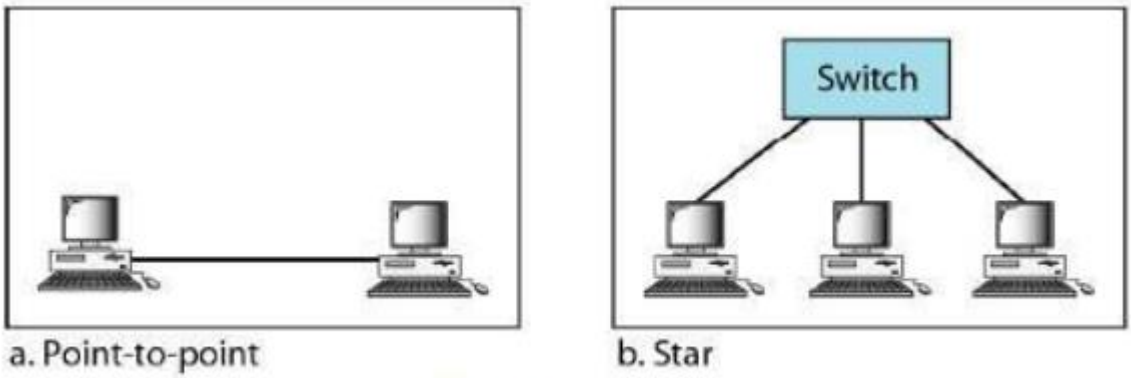


Figure 13.19 *Fast Ethernet topology*

Table 13.2 *Summary of Fast Ethernet implementations*

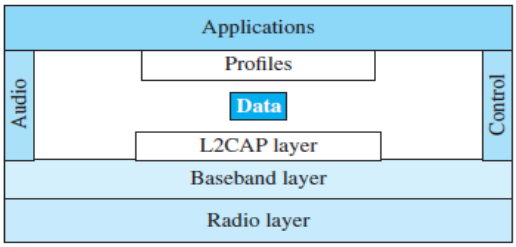
Implementation	*Medium*	*Medium Length*	*Wires*	*Encoding*
100Base-TX	UTP or STP	100 m	2	4B5B + MLT-3
100Base-FX	Fiber	185 m	2	4B5B + NRZ-I
100Base-T4	UTP	100 m	4	Two 8B/6T

Encoding

There are 3 different encoding schemes.
100Base-TX
100Base-FX
100Base-T4

4b) Explain the different layers of Bluetooth Network.

Figure 15.19 *Bluetooth layers*



L2CAP

- The **Logical Link Control and Adaptation Protocol,** or **L2CAP** (L2 here means LL), is roughly equivalent to the LLC sublayer in LANs.
- It is used for data exchange on an ACL link; SCO channels do not use L2CAP.

Figure 15.20 *L2CAP data packet format*

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

- The L2CAP has specific duties :

1) Multiplexing:

- At the sender site, it accepts data from one of the upper-layer protocols, frames them, and delivers them to the baseband layer.
- At the receiver site, it accepts a frame from the baseband layer, extracts the data, and delivers them to the appropriate protocol layer segmentation and reassembly, quality of service (QoS), and group management.

2) Segmentation and Reassembly

- The maximum size of the payload field in the baseband layer is 2774 bits, or 343 bytes. This includes 4 bytes to define the packet and packet length.
- the size of the packet that can arrive from an upper layer can only be 339 bytes.
- The 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 packets at the source and reassembles them at the destination.

3) QoS

4) Group Management: L2CAP is to allow devices to create a type of logical addressing between themselves. This is similar to multicasting

Baseband Layer

- The access method is TDMA
- The primary and secondary stations communicate with each other using time slots. The length of a time slot is exactly the same as the dwell time, 625 μs. This means that during the time that one frequency is used, a primary sends a frame to a secondary, or a secondary sends a frame to the primary.
- ***TDMA :*** Bluetooth uses a form of TDMA that is called ***TDD-TDMA (time-division duplex TDMA).***

- TDD-TDMA is a kind of half-duplex communication in which the sender and receiver send and receive data, but not at the same time (half-duplex); however, the communication for each direction uses different hops.

- ***Links*** Two types of links can be created between a primary and a secondary:.
  i) SCO A **synchronous connection-oriented (SCO) link** is

- ❖ used when avoiding latency is more important than integrity (error-free delivery).
- ❖ In an SCO link, a physical link is created between the primary and a secondary by reserving specific slots at regular intervals.
- ❖ The basic unit of connection is two slots, one for each direction. If a packet is damaged, it is never retransmitted.

ii) ***ACL*** An **asynchronous connectionless link (ACL)** is

- used when data integrity is more important than avoiding latency.
- In this type of link, if a payload encapsulated in the frame is corrupted, it is retransmitted.
- A secondary returns an ACL frame in the available odd-numbered slot if the previous slot has been addressed to it.
- ACL can use one, three, or more slots and can achieve a maximum data rate of 721 kbps.

Radio Layer

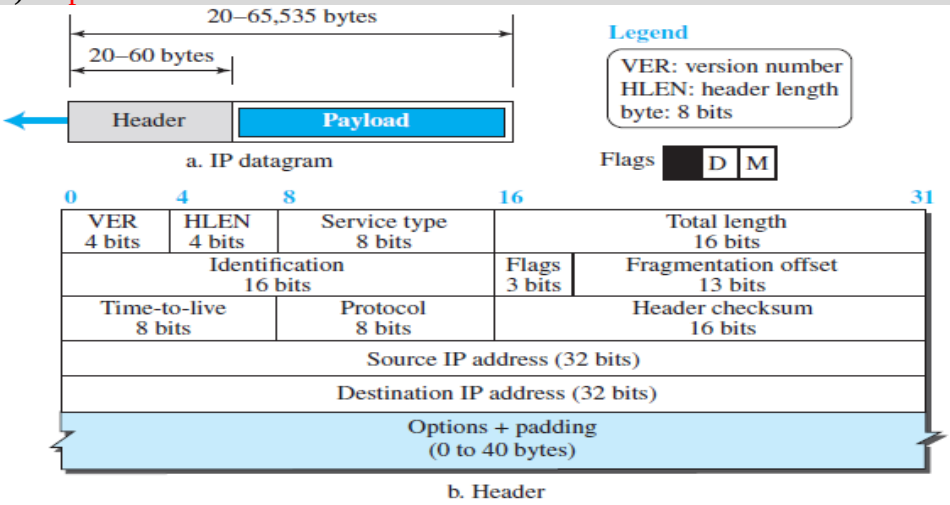
- The radio layer is roughly equivalent to the physical layer of the Internet model. Bluetooth devices are low-power and have a range of 10 m.
- ***Band :*** Bluetooth uses a 2.4-GHz ISM band divided into 79 channels of 1 MHz each.
- ***FHSS:*** Bluetooth uses the **frequency-hopping spread spectrum (FHSS)** method in the physical

layer to avoid interference from other devices or other networks. Bluetooth hops 1600 times per second, which means that each device changes its modulation frequency 1600 times per second. A device uses a frequency for only 625µ s (1/1600 s) before it hops to another frequency; the dwell time is 625µs.

- ***Modulation:***

To transform bits to a signal, Bluetooth uses a sophisticated version of FSK, called GFSK (FSK with Gaussian bandwidth filtering;
GFSK has a carrier frequency. Bit 1 is represented by a frequency deviation above the carrier; bit 0 is represented by a frequency deviation below the carrier.
The frequencies, in megahertz, are defined according to the following formula for each channel.

5a) Explain in detail IPV4 header format.



❑***Version Number.*** The 4-bit version number (VER) field defines the version of the IPv4 protocol, which, obviously, has the value of 4.

❑***Header Length.*** The 4-bit header length (HLEN) field defines the total length of the datagram header in 4-byte words. The IPv4 datagram has a variable-length header.

- ❖ to make the value of the header length (number of bytes) fit in a 4-bit header length, the total length of the header is calculated as 4-byte words. The total length is divided by 4 and the value is inserted in the field. The receiver needs to multiply the value of this field by 4 to find the total length.

❑ ***Service Type*.** In the original design of the IP header, this field was referred to as type of service (TOS), which defined how the datagram should be handled.

- IETF redefined the field to provide *differentiated services* (DiffServ).

❑***Total Length*.**

- This 16-bit field defines the total length (header plus data) of the IP datagram in bytes. A 16-bit number can define a total length of up to 65,535
- This field helps the receiving device to know when the packet has completely arrived. To find the length of the data coming from the upper layer, subtract the header length from the total length. The header length can be found by multiplying the value in the HLEN field by 4.
- $\text{Length of data} = \text{total length} - (\text{HLEN}) \times 4$

❑***Identification, Flags, and Fragmentation Offset*.**

- These three fields are related to the fragmentation of the IP datagram when the size of the datagram is larger than the underlying network can carry.

❑***Time-to-live*.**

- Due to some malfunctioning of routing protocols a datagram may be circulating in the Internet, visiting some networks over and over without reaching the destination. This may create extra traffic in the Internet.
- The time-to-live (TTL) field is used to control the maximum number of hops (routers) visited by the datagram.
- When a source host sends the datagram, it stores a number in this field. This value is approximately two times the maximum number of routers between any two hosts. Each router that processes the datagram decrements this number by one. If this value, after being decremented, is zero, the router discards the datagram.

❑***Protocol*.**

- In TCP/IP, the data section of a packet, called the *payload*, carries the whole packet from another protocol. A datagram, for example, can carry a packet belonging to any transport-layer protocol such as UDP or TCP.
- A datagram can also carry a packet from other protocols that directly use the service of the IP, such as some routing protocols or some auxiliary protocols.
- This field provides multiplexing at the source and demultiplexing at the destination

❑***Header checksum*.**

- IP is not a reliable protocol; it does not check whether the payload carried by a datagram is corrupted during the transmission.

- For example, if the destination IP address is corrupted, the packet can be delivered to the wrong host. If the protocol field is corrupted, the payload may be delivered to the wrong protocol. If the fields related to the fragmentation are corrupted, the datagram cannot be reassembled correctly at the destination, and so on. For these reasons, IP adds a header checksum field to check the header, but not the payload.

❑***Source and Destination Addresses*.**

- These 32-bit source and destination address fields define the IP address of the source and destination respectively.
- The source host should know its IP address.
- The destination IP address is either known by the protocol that uses the service of IP or is provided by the DNS

❑***Options.***

- A datagram header can have up to 40 bytes of options. Options can be used for network testing and debugging.
- The existence of options in a header creates some burden on the datagram handling; some options can be changed by routers, which forces each router to recalculate the header checksum. There are one-byte and multi-byte options.

❑***Payload*.**

- Payload, or data, is the main reason for creating a datagram.
- Payload is the packet coming from other protocols that use the service of IP.

b)

Extension Header

An IP packet is made of base-header &
some extension headers.

Length of base header = 40 bytes.

To support extra functionalities, extension headers can be placed b/w base header and payload.

Extension headers act like options in IPv4.
Six types of extension headers (Figure 22.8):

1)	Hop-by-hop option	2)	Source routing	3)	Fragmentation
4)	Authentication	5)	Encrypted security payload	5)	Destination option.

6) List and explain 3different categories of Satellites.

Three Categories of Satellites
• Three categories of satellites based on the location of the orbit (Figure 16.18):
1) Geostationary Earth orbit (GEO)
There is only one orbit, at an altitude of 36000 km, for the GEO satellite.☐

2) Low-Earth-orbit (LEO)
LEO satellites are below an altitude of 2000 km.☐

3) Medium-Earth-orbit (MEO)

MEO satellites are located at altitudes between 5000 and 15,000 km.

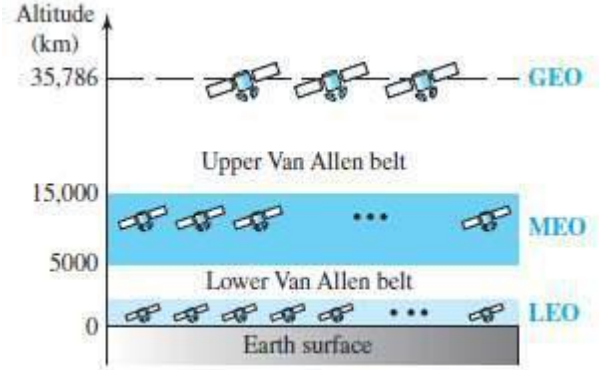


Figure 16.18 *Satellite orbit altitudes*

GEO Satellites
There is only one orbit at an altitude of 36,000 km (Figure 16.19).

Because orbital speed is based on the distance from the planet, only one orbit can be geostationary.

The orbit occurs at the equatorial plane.
Sending-antenna must have receiving-antenna in LOS (Line-of-sight).

Problem: A satellite that moves faster/slower than Earth"s rotation is useful only for short periods. Solution: To ensure constant communication, the satellite must move at same speed as the Earth.

Thus, the satellite seems to remain fixed above a certain spot.

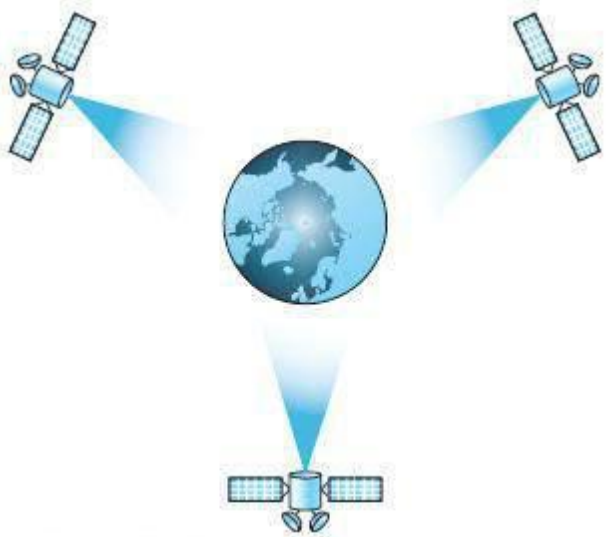


Figure 16.19 *Satellites in geostationary orbit*

MEO Satellites

MEO satellites are located at altitudes between 5000 and 15,000 km.

Example: Global Positioning System (GPS)

Global Positioning System

GPS consists of 24 satellites in 6 orbits (Figure 16.20).

GPS is used for land, sea, and air navigation to provide time and location for vehicles and ships.

The orbits and the locations of the satellites in each orbit are designed systematically.

For example: At any time, 4 satellites are visible from any point on Earth.

• A GPS receiver has an almanac (or calendar) that tells the current position of each satellite.

Here we discuss, 4 issues:

1) Trilateration 2) Measuring the Distance

3) Synchronization 4) Application

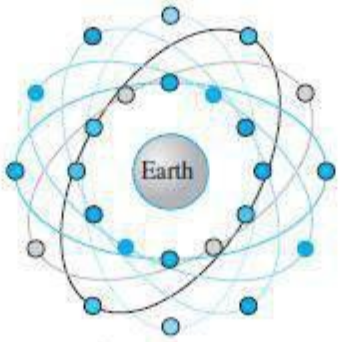


Figure 16.20 *Orbits for global positioning system (GPS) satellites*

LEO Satellites

LEO satellites have polar orbits.

Usually, a LEO system has a cellular type of access (similar to the cellular telephone system).

Specifications:

Altitude = 500 to 2000 km
Rotation Period = 90 to 120 min
Satellite Speed =20,000 to 25,000 km/h
Footprint Diameter = 8000 km
Round-Trip Time < 20 ms
Because LEO satellites are close to Earth, 20 ms RTT is normally acceptable for audio communication.

A LEO system is made of a group of satellites that work together as a network.

Each satellite acts as a switch.
Different types of links (Figure 16.22):

1) ISLs (Inter-Satellite Links)
Satellites that are close to each other are connected through ISLs.☐

2) UML (User Mobile Link)
A mobile system communicates with the satellite through a UML.☐

3) GWL (Gate Way Link)
A satellite communicates with the Earth station (gateway) through a GWL.

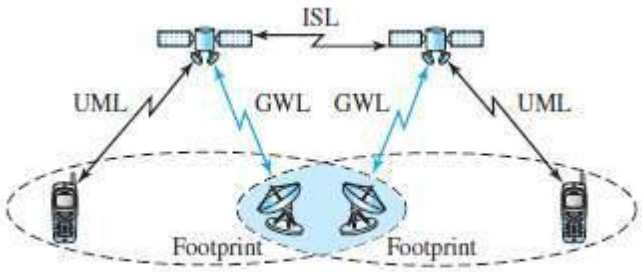


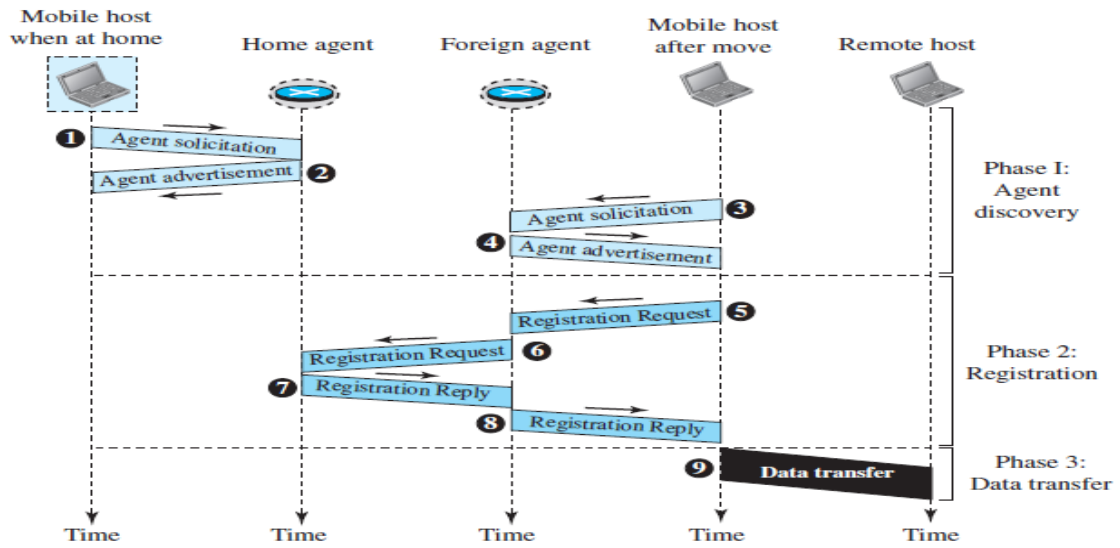
Figure 16.22 *LEO satellite system*

LEO satellites can be divided into three categories:
1) Little LEO
2) Big LEO
3) Broadband LEO

7a) Explain the three phase communication process between remote host and mobile host.

To communicate with a remote host, a mobile host goes through three phases: agent discovery, registration, and data transfer.

Figure 19.14 *Remote host and mobile host communication*



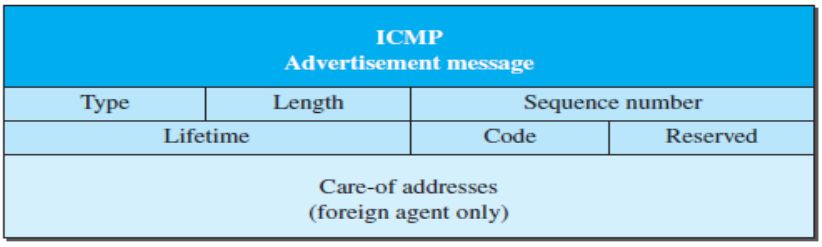
Agent Discovery

- The first phase in mobile communication, *agent discovery*, consists of two sub phases.
- A mobile host must discover (learn the address of) a home agent before it leaves its home network.
- A mobile host must also discover a foreign agent after it has moved to a foreign network. This discovery consists of learning the care-of address as well as the foreign agent's address.
- The discovery involves two types of messages: advertisement and solicitation.

i) Agent Advertisement

- When a router advertises its presence on a network using an ICMP router advertisement, it can append an *agent advertisement* to the packet if it acts as an agent.

Figure 19.15 *Agent advertisement*



The field descriptions are as follows:

❑***Type.*** The 8-bit type field is set to 16.

❑***Length.*** The 8-bit length field defines the total length of the extension message

❑***Sequence number.*** The 16-bit sequence number field holds the message number. The recipient can use the sequence number to determine if a message is lost.

❑***Lifetime.*** The lifetime field defines the number of seconds that the agent will accept requests. If the value is a string of 1s, the lifetime is infinite.

❑***Code.*** The code field is an 8-bit flag in which each bit is set (1) or unset (0).

❑***Care-of Addresses.*** This field contains a list of addresses available for use as care of addresses. The mobile host can choose one of these addresses. The selection of this care-of address is announced in the registration request.

Agent Solicitation

When a mobile host has moved to a new network and has not received agent advertisements, it can initiate an *agent solicitation.* It can use the ICMP solicitation message to inform an agent that it needs assistance.

i) Registration

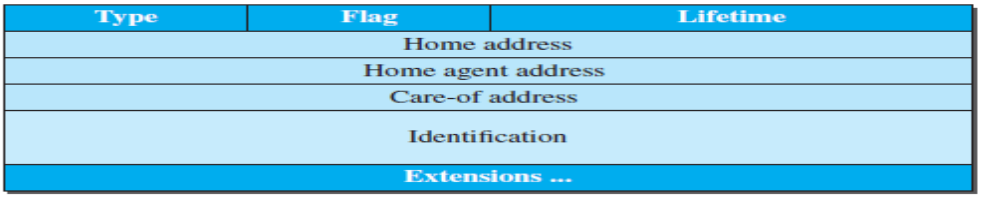
The second phase in mobile communication is *registration*. After a mobile host has moved to a foreign network and discovered the foreign agent, it must register. There are four aspects of registration:
1. The mobile host must register itself with the foreign agent.
2. The mobile host must register itself with its home agent. This is normally done by the foreign agent on behalf of the mobile host.
3. The mobile host must renew registration if it has expired.
4. The mobile host must cancel its registration (deregistration) when it returns home.

Request and Reply

To register with the foreign agent and the home agent, the mobile host uses a *registration request* and a registration reply

ii)Registration Request A registration request is sent from the mobile host to the foreign agent to register its care-of address and also to announce its home address and home agent address. The foreign agent, after receiving and registering the request ,relays the message to the home agent. Note that the home agent now knows the address of the foreign agent because the IP packet that is used for relaying has the IP address ofthe foreign agent as the source address.

Figure 19.16 *Registration request format*

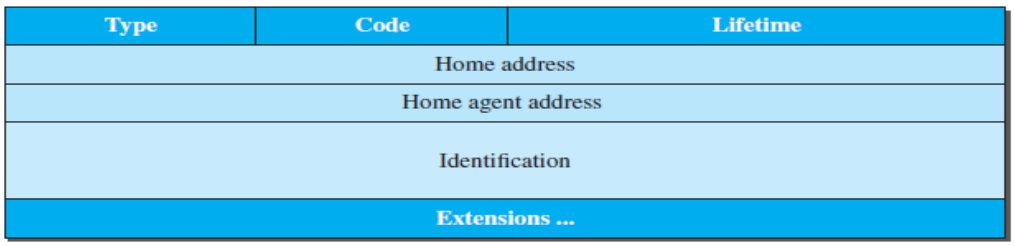


The field descriptions are as follows:

- ***Type.*** The 8-bit type field defines the type of message. For a request message the value of this field is 1.
- ***Flag.*** The 8-bit flag field defines forwarding information. The value of each bit can be set or unset.
- ***Lifetime.*** This field defines the number of seconds the registration is valid. If the field is a string of 0s, the request message is asking for deregistration. If the field is a string of 1s, the lifetime is infinite.
- ***Home address.*** This field contains the permanent (first) address of the mobile host.
- ***Home agent address.*** This field contains the address of the home agent.
- ***Care-of address.*** This field is the temporary (second) address of the mobile host.
- ***Identification.*** This field contains a 64-bit number that is inserted into the request by the mobile host and repeated in the reply message. It matches a request with a reply.
- ***Extensions.*** Variable length extensions are used for authentication. They allow a home agent to authenticate the mobile agent.

Registration Reply A registration reply is sent from the home agent to the foreign agent and then relayed to the mobile host. The reply confirms or denies the registration request.

Figure 19.17 *Registration reply format*



Encapsulation

Registration messages are encapsulated in a UDP user datagram. An agent uses the well-known port 434; a mobile host uses an ephemeral port.

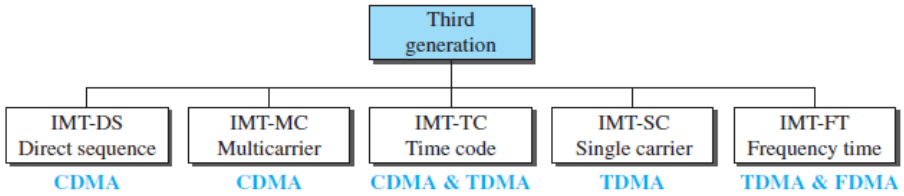
Data Transfer

After agent discovery and registration, a mobile host can communicate with a remote host.

7b) Write short note on 3G systems

- The third generation of cellular telephony refers to a combination of technologies that provide both digital data and voice communication.
- **The main goal of third-generation cellular telephony is to provide universal personal communication.**
- Criteria for third-generation technology.
  - Voice quality comparable to that of the existing public telephone network.
  - Data rate of 144 kbps for access in a moving vehicle (car), 384 kbps for access as the user walks (pedestrians), and 2 Mbps for the stationary user (office or home).
  - Support for packet-switched and circuit-switched data services.
  - A band of 2 GHz, Bandwidths of 2 MHz.
  - Interface to the Internet

Figure 16.16 *IMT-2000 radio interfaces*



IMT-2000 Radio Interfaces

- Figure shows the radio interfaces (wireless standards) adopted by IMT-2000. All five are developed from second-generation technologies. The first two evolve from CDMA technology. The third evolves from a combination of CDMA and TDMA. The fourth evolves from TDMA, and the last evolves from both FDMA and TDMA.

IMT-DS

- This approach uses a version of CDMA called *wideband CDMA* or *W-CDMA*.
- W-CDMA uses a 5-MHz bandwidth.

IMT-MC

- This approach was developed in North America and is known as *CDMA 2000*.
- It is an evolution of CDMA technology used in IS-95 channels. It combines the new wideband
- (15-MHz) spread spectrum with the narrowband (1.25-MHz) CDMA of IS-95.
- It is backward-compatible with IS-95. It allows communication on multiple 1.25-MHz
- channels (1, 3, 6, 9, 12 times), up to 15 MHz.

IMT-TC

- This standard uses a combination of W-CDMA and TDMA.
- The standard tries to reach the IMT-2000 goals by adding TDMA multiplexing to W-CDMA.

IMT-SC

- This standard uses only TDMA.

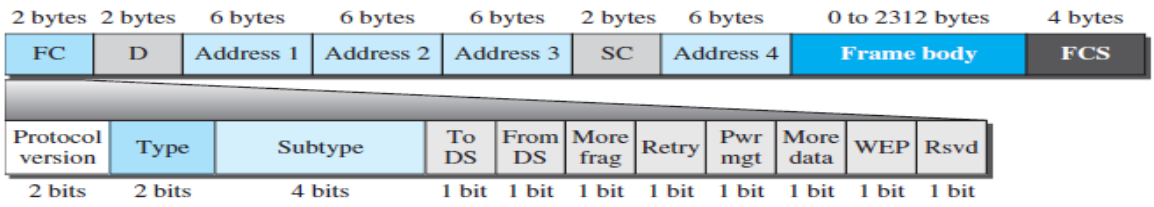
IMT-FT

- This standard uses a combination of FDMA and TDMA.

8) Explain the MAC 802.11 frame format.

The MAC layer frame consists of nine fields,

Figure 15.9 *Frame format*



- ***Frame control (FC).*** The FC field is 2 bytes long and defines the type of frame and some control information.

Subfields in FC field

Field	Explanation
Version	Current version is 0
Type	Type of information: management (00), control (01), or data (10)
Subtype	Subtype of each type (see Table 15.2)
To DS	Defined later
From DS	Defined later
More frag	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 management mode
More data	When set to 1, means station has more data to send
WEP	Wired equivalent privacy (encryption implemented)
Rsvd	Reserved

- ***D.*** This field defines the duration of the transmission that is used to set the value of NAV. In one control frame, it defines the ID of the frame.
- ***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* subfields
- ***Sequence control.*** This field, often called the *SC* field, defines a 16-bit value. The first four bits define the fragment number; the last 12 bits define the sequence number, which is the same in all fragments.
- ***Frame body.*** This field, which can be between 0 and 2312 bytes, contains information based on the type and the subtype defined in the FC field.
- ***FCS.*** The FCS field is 4 bytes long and contains a CRC-32 error-detection sequence

Frame Types

A wireless LAN defined by IEEE 802.11 has three categories of frames:]

- Management frames,
- control frames,
- and data frames.

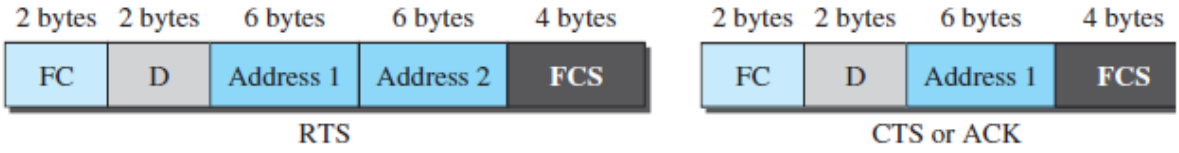
Management Frames

Management frames are used for the initial communication between stations and access points.

Control Frames

Control frames are used for accessing the channel and acknowledging frames

Figure 15.10 *Control frames*



For control frames the value of the type field is 01; the values of the subtype fields for frames

Table 15.2 *Values of subtype fields in control frames*

Subtype	Meaning
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

Data Frames

Data frames are used for carrying data and control information.