CMR INSTITUTE OF TECHNOLOGY

USN | | | | | | | | | | |

Internal Assesment Test – III – May 2017

Sub:	DATA COMMUNICATIONS							Code:	15CS46
Date:	29 / 05 / 2017	Duration:	90 mins	Max Marks:	50	Sem:	IV B/C/D	Branch:	ISE

Answer Any FIVE FULL Questions

		CO	RBT
1.	Explain the architecture of IEEE 802.11 standards. [10]	CO4	L3
2.	In detail, explain the hidden and exposed station problem in IEEE 802.11. [10]	CO4	L3
3.	Explain in detail the architecture of Bluetooth. [10]	CO4	L3
4.	Explain IPV4 header format. [10]	CO5	L3
5.	Explain the three phase communication process between remote host and mobile host. [10]	CO5	L3
6.	Write a short note on a) 3G [5]	CO5	L2
	b) GSM [5]	CO5	L2
7.	Explain in detail the Cellular Telephony(Frequency reuse, Handoff, Roaming concept) [10]	CO4	L3
8.	Explain the Frame format of IEEE 802.16. [10]	CO5	L3

----------ALL THE BEST ----------

CMR INSTITUTE OF TECHNOLOGY

USN | | | | | | | | | | |

Internal Assesment Test – III – May 2017

Sub:	DATA COMMUNICATIONS							Code:	15CS46
Date:	29 / 05 / 2017	Duration:	90 mins	Max Marks:	50	Sem:	IV B/C/D	Branch:	ISE

Answer Any FIVE FULL Questions

		CO	RBT
9.	Explain the architecture of IEEE 802.11 standards. [10]	CO4	L3
10.	In detail, explain the hidden and exposed station problem in IEEE 802.11. [10]	CO4	L3
11.	Explain in detail the architecture of Bluetooth. [10]	CO4	L3
12.	Explain IPV4 header format. [10]	CO5	L3
13.	Explain the three phase communication process between remote host and mobile host. [10]	CO5	L3
14.	Write a short note on a) 3G [5]	CO5	L2
	b) GSM [5]	CO5	L2
15.	Explain in detail the Cellular Telephony(Frequency reuse, Handoff, Roaming concept) [10]	CO4	L2
16.	Explain the Frame format of IEEE 802.16. [10]	CO5	L3

----------ALL THE BEST ----------

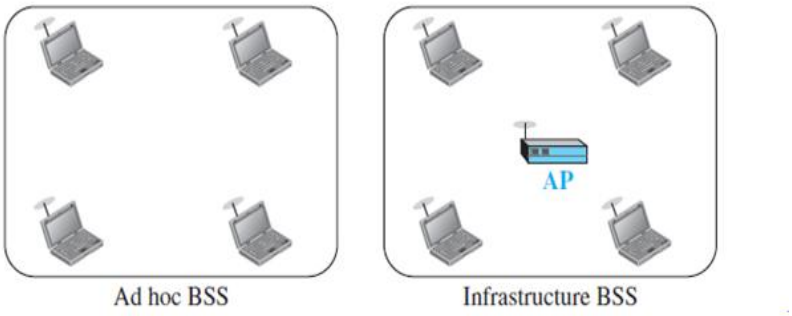
1. Explain the architecture of IEEE 802.11 standards.

The standard defines two kinds of services:

- the basic service set (BSS)
- the extended service set (ESS).

i) Basic Service Set

- IEEE 802.11 defines the **basic service set (BSS)** as the building blocks of a wireless LAN.
- It is made of stationary or mobile wireless stations and an optional central base station(*access point (AP)).*



- The BSS without an AP is a stand-alone network and cannot send data to other BSSs. It is called an *ad hoc architecture*.
- Stations can form a network without the need of an AP; they can locate one another and agree to be part of a BSS.
- A BSS with an AP is sometimes referred to as an *infrastructure BSS*.

ii) Extended Service Set

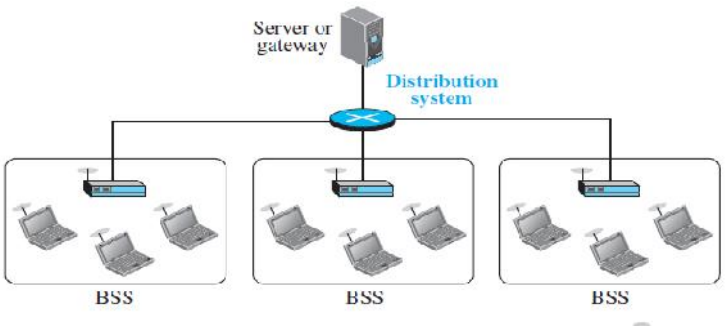
It is made up of two or more BSSs with APs.

- the BSSs are connected through a *distribution system,* which is a wired or a wireless network
- The distribution system connects the APs in the BSSs.
- The extended service set 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.

When BSSs are connected, the stations within reach of one another can communicate without the use of an AP.



iii) Station Types

IEEE 802.11 defines three types of stations based on their mobility in a wireless LAN

- no-transition,
- BSS-transition,
- ESS-transition mobility.

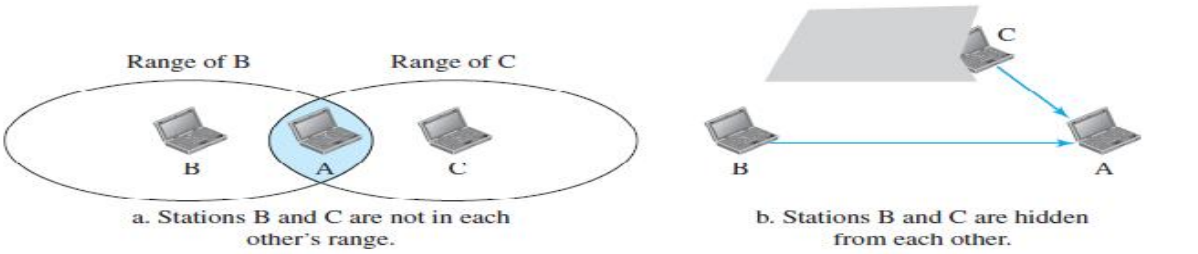
A station with **no-transition mobility** is either stationary (not moving) or moving only inside a BSS.

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.

2) Explain in detail about the hidden and exposed station problem in IEEE 802.11

Hidden-Station Problem
In which a station may not be aware of another station's transmission due to some obstacles or range problems, collision may occur but not be detected.
Figure shows an example of the hidden station problem.

Figure 15.3 *Hidden station problem*

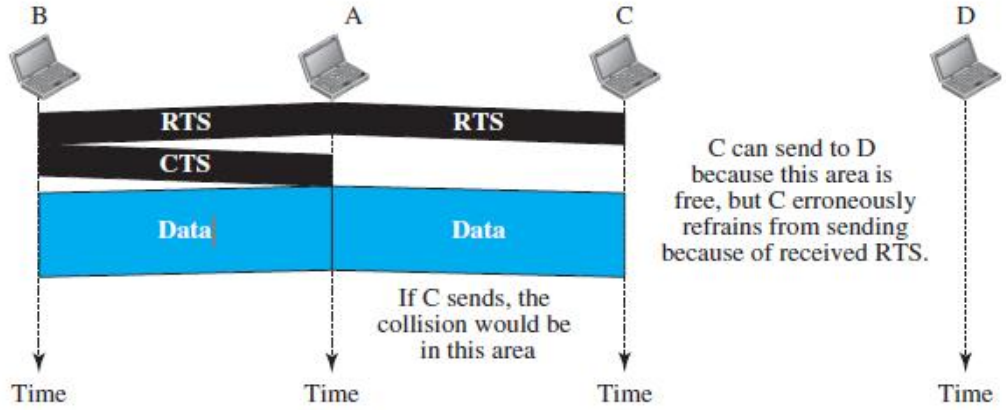


- Station B has a transmission range shown by the left oval (sphere inspace); every station in this range can hear any signal transmitted by station B.
- Station C has a transmission range shown by the right oval (sphere in space); every station located in this range can hear any signal transmitted by C.
- Station C is outside the transmission range of B; likewise, station B is outside the transmission range of C.
- Station A, however, is in the area covered by both B and C; it can hear any signal transmitted by B or C.
- The figure also shows that the hidden station problem may also occur due to an obstacle.
- Assume that station B is sending data to station A. In the middle of this transmission, station C also has data to send to station A. However, station C is out of B's range and transmissions from B cannot reach C. Therefore C thinks the medium is free. Station C sends its data to A, which results in a collision at A because this station is receiving data from both B and C. In this case, we say that stations B and C are hidden from each other with respect to A.
- Hidden stations can reduce the capacity of the network because of the possibility of collision.
- The solution to the hidden station problem is the use of the handshake frames (RTS and CTS).

Exposed Station Problem

- In this problem a station refrains from using a channel when it is, in fact, available.
- In the below Figure station A is transmitting to station B. Station C has some data to send to station D, which can be sent without interfering with the transmission from A to B.
- However, station C is exposed to transmission from A; it hears what A is sending and thus refrains from sending.
- In other words, C is too conservative and wastes the capacity of the channel. The handshaking messages RTS and CTS cannot help in this case.
- Station C hears the RTS from A and refrains from sending, even though the communication between C and D cannot cause a collision in the zone between A and C; station C cannot know that station A' transmission does not affect the zone between C and D.

Figure 15.12 *Exposed station problem*

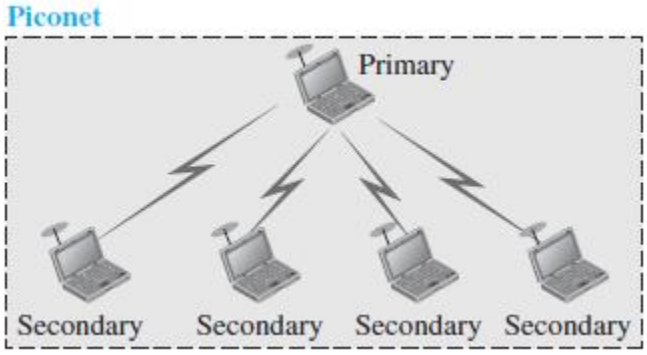


3) Explain the Bluetooth architecture in detail.

Bluetooth defines two types of networks: piconet and scatternet.

i) Piconets

- A Bluetooth network is called a ***piconet,*** or a small net.
- A piconet can have up to eight stations, one of which is called the *primary;* the rest are called *secondaries.*
- All the secondary stations synchronize their clocks and hopping sequence with the primary.
- The communication between the primary and secondary stations can be one-to-one or one-to-many.

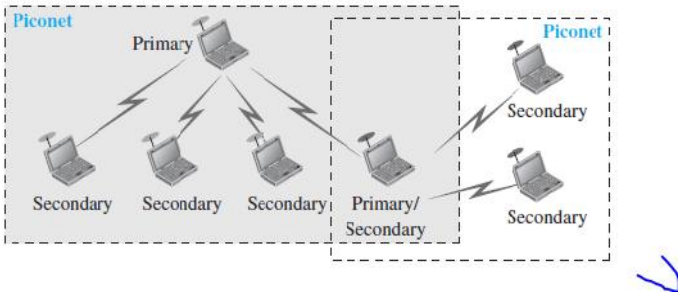


- Although a piconet can have a maximum of seven secondaries, additional secondaries can be in the *parked state*.
- A secondary in a parked state is synchronized with the primary, but cannot take part in communication until it is moved from the parked state to the active state. Because only eight stations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

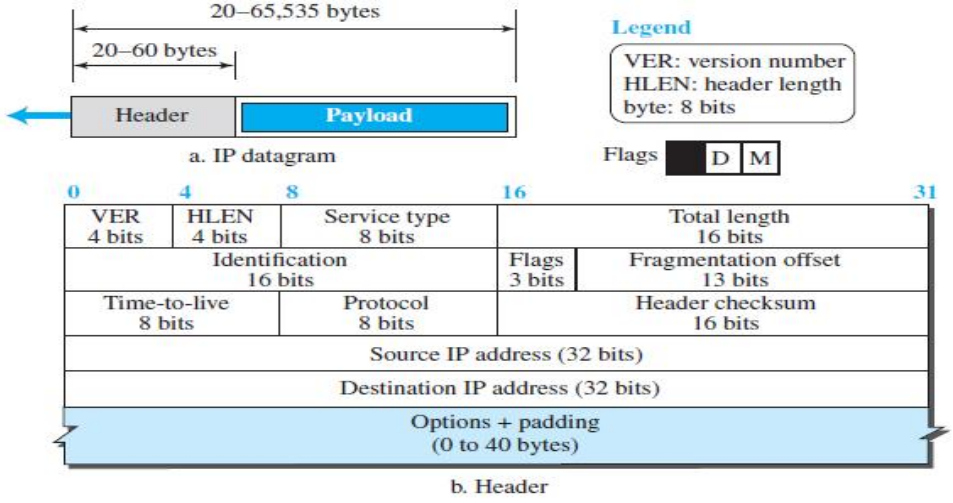
ii) Scatternet

- Piconets can be combined to form a ***scatternet.***
- A secondary station in one piconet can be the primary in another piconet. This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliverthem to secondaries in the second piconet.
- A station can be a member of two piconets.

Figure 15.18 *Scatternet*



4) 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.

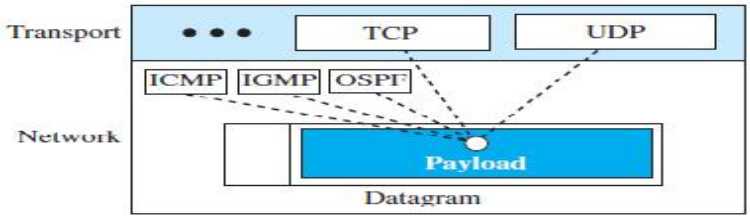
❑ ***Time-to-live.***

- 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

Figure 19.3 *Multiplexing and demultiplexing using the value of the protocol field*



Some protocol values

ICMP	01
IGMP	02
TCP	06
UDP	17
OSPF	89

❑ ***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.

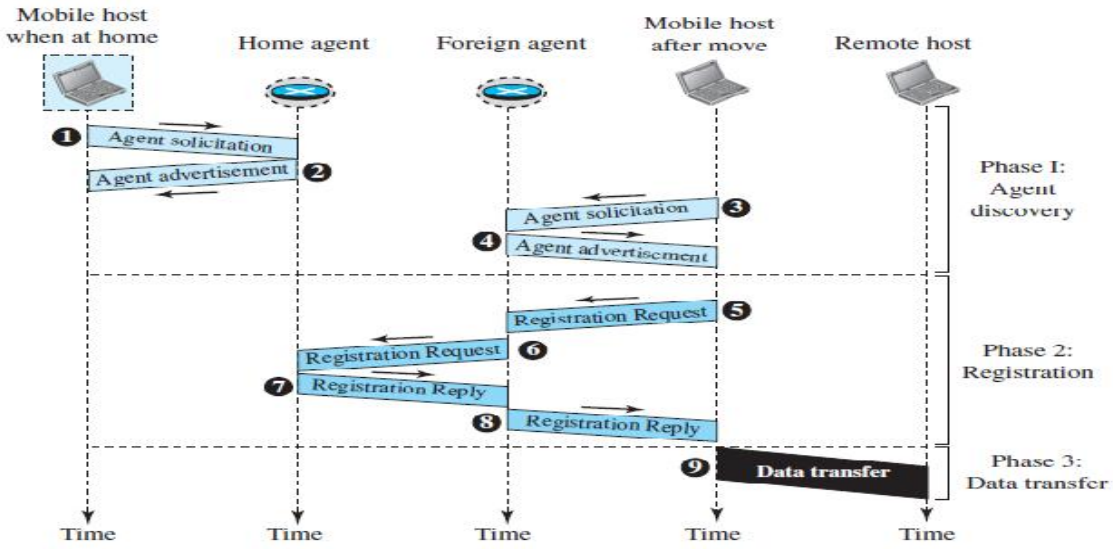
❑ ***Payload.***

- ❖ 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.

5) 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*



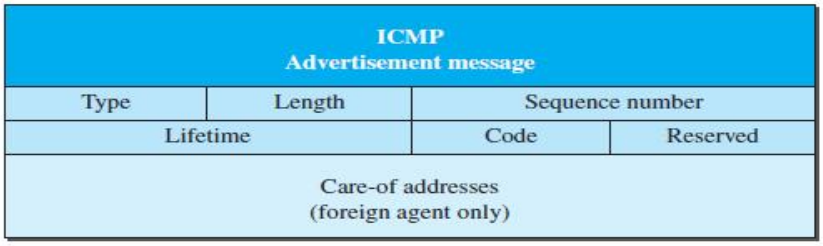
Agent Discovery

- 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:

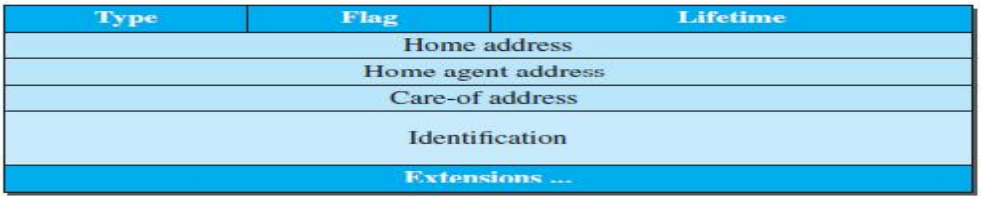
1. The mobile host must register itself with the foreign agent.
2. The mobile host must register itself with its home agent. This is normally done by the foreign agent on behalf of the mobile host.
3. The mobile host must renew registration if it has expired.
4. The mobile host must cancel its registration (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*

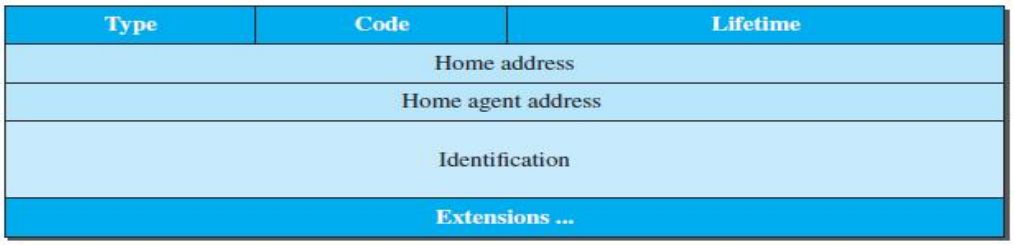


The field descriptions are as follows:

- ***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.

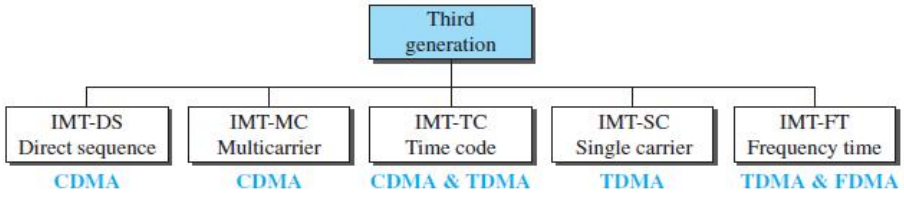
6a) Write short note on 3G systems

- 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.**

- Using a small portable device, a person is able to talk to anyone else in the world with a voice quality similar to that of the existing fixed telephone network.
- A person can download and watch a movie, download and listen to music, surf the Internet or play games, have a video conference.
- 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.

6b) Write short note on GSM

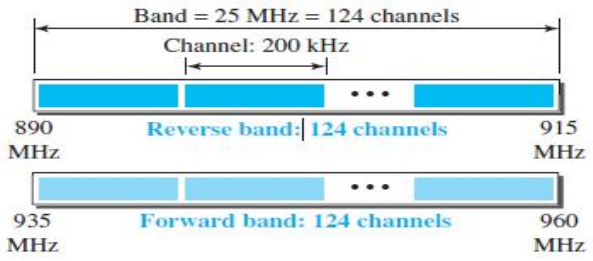
- The **Global System for Mobile Communication (GSM)** is a European standard that was developed to provide a common second-generation technology for all Europe.
- The aim was to replace a number of incompatible first-generation technologies

.

Bands

- GSM uses two bands for duplex communication. Each band is 25 MHz in width, shifted toward 900 MHz, as shown in Figure . Each band is divided into 124 channels of 200 kHz separated by guard bands.

gure 16.11 *GSM bands*



Transmission

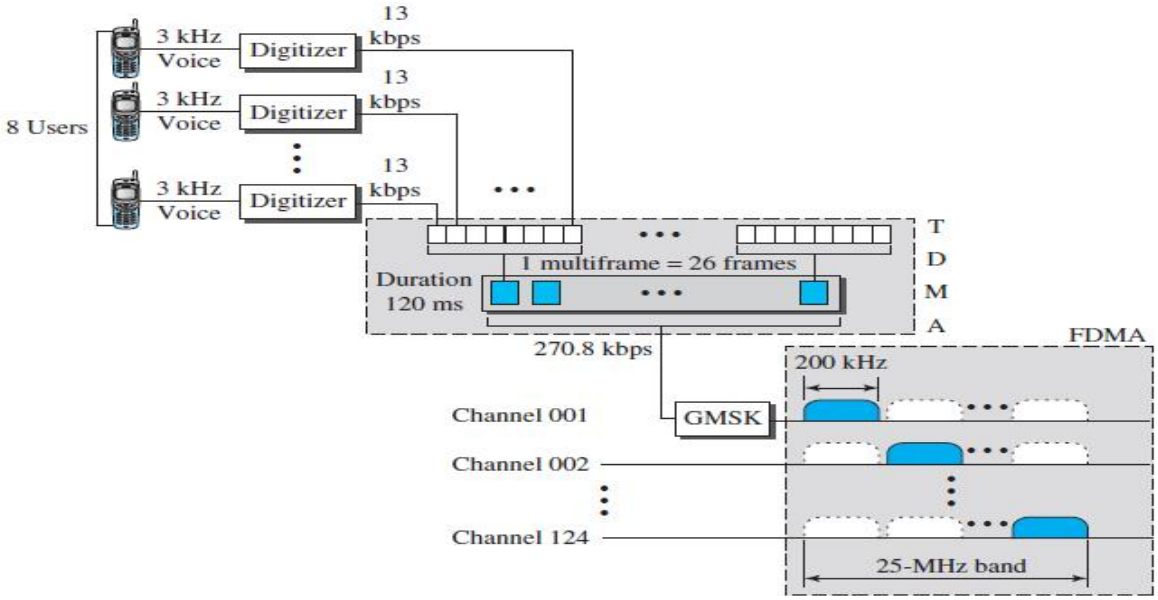
- Each voice channel is digitized and compressed to a 13-kbps digital signal. Each slot carries 156.25 bits. Eight slots share a frame (TDMA).
- Twenty-six frames also share a multiframe (TDMA).

We can calculate the bit rate of each channel as follows.

- Each 270.8-kbps digital channel modulates a carrier using GMSK the result is a 200-kHz analog signal. Finally 124 analog channels of 200 kHz are combined using FDMA. The result is a 25-MHz band. Figure shows the user data and overhead in a multiframe.

$$\text{Channel data rate} = (1/120\ \text{ms}) \times 26 \times 8 \times 156.25 = 270.8\ \text{kbps}$$

Figure 16.12 *GSM*



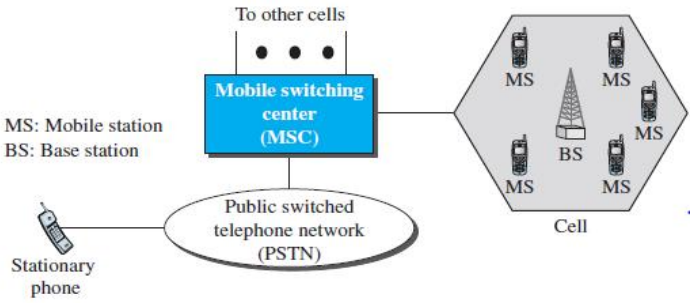
Reuse Factor

- Because of the complex error correction mechanism, GSM allows a reuse factor as low as 3.
- **GSM is a digital cellular phone system using TDMA and FDMA.**

7) Explain in detail about Cellular Telephony(Frequency reuse,Handoff,Roaming concept)

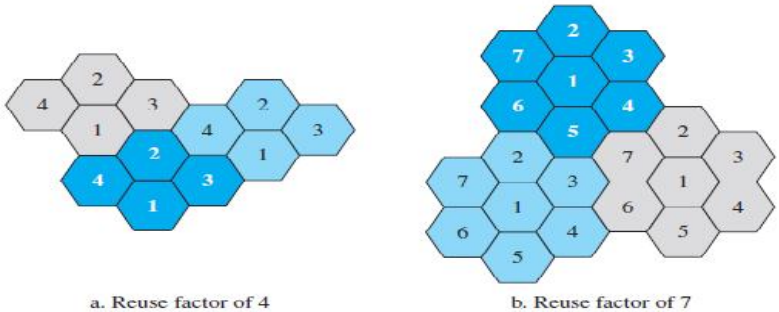
- Designed to provide communications between two moving units, called *mobile stations (MSs)*, or between one mobile unit and one stationary unit, often called a *land unit*.
- A service provider must be able to locate and track a caller, assign a channel to the call, and transfer the channel from base station to base station as the caller moves out of range.
- Each cellular service area is divided into small regions called *cells*.
- Each cell contains an antenna and is controlled by a solar- or AC powered network station, called the *base station* (BS).
- Each base station, in turn, is controlled by a switching office, called a ***mobile switching center (MSC).***
- The MSC coordinates communication between all the base stations and the telephone central office.

'igure 16.6 *Cellular system*



- The operation of the cellular telephony:
  i) ***Frequency-Reuse Principle:***
    - ❖ neighboring cells cannot use the same set of frequencies for communication because doing so may create interference for the users located near the cell boundaries.
    - ❖ the set of frequencies available is limited, and frequencies need to be reused.
    - ❖ A frequency reuse pattern is a configuration of *N* cells, *N* being the **reuse factor,** in which each cell uses a unique set of frequencies.
    - ❖ When the pattern is repeated, the frequencies can be reused. There are several different patterns.
    - ❖ The numbers in the cells define the pattern.
    - ❖ The cells with the same number in a pattern can use the same set of frequencies. We call these cells the *reusing cells*.

Figure 16.7 *Frequency reuse patterns*



ii) Transmitting

- ❖ To place a call from a mobile station, the caller enters a code of 7 or 10 digits (a phone number) and presses the send button.
- ❖ The mobile station then scans the band, seeking a setup channel with a strong signal, and sends the data (phone number) to the closest base station using that channel.

- The base station relays the data to the MSC. The MSC sends the data on to the telephone central office. If the called party is available, a connection is made and the result is relayed back to the MSC.
- At this point, the MSC assigns an unused voice channel to the call, and a connection is established. The mobile station automatically adjusts its tuning to the new channel, and communication can begin.

iii) Receiving

- When a mobile phone is called, the telephone central office sends the number to the MSC.
- The MSC searches for the location of the mobile station by sending query signals to each cell in a process called *paging*.
- Once the mobile station is found, the MSC transmits a ringing signal and, when the mobile station answers, assigns a voice channel to the call, allowing voice communication

iv) Handoff

- It may happen that, during a conversation, the mobile station moves from one cell to another.
- When it does, the signal may become weak. To solve this problem, the MSC monitors the level of the signal every few seconds. If the strength of the signal diminishes, the MSC seeks a new cell that can better accommodate the communication.
- The MSC then changes the channel carrying the call

Hard Handoff

- In a hard handoff, a mobile station only communicates with one base station. When the MS moves from one cell to another, communication must first be broken with the previous base station before communication can be established with the new one. This may create a rough transition.

Soft Handoff

- In this case, a mobile station can communicate with two base stations at the same time. This means that, during handoff, a mobile station may continue with the new base station before breaking off from the old one.

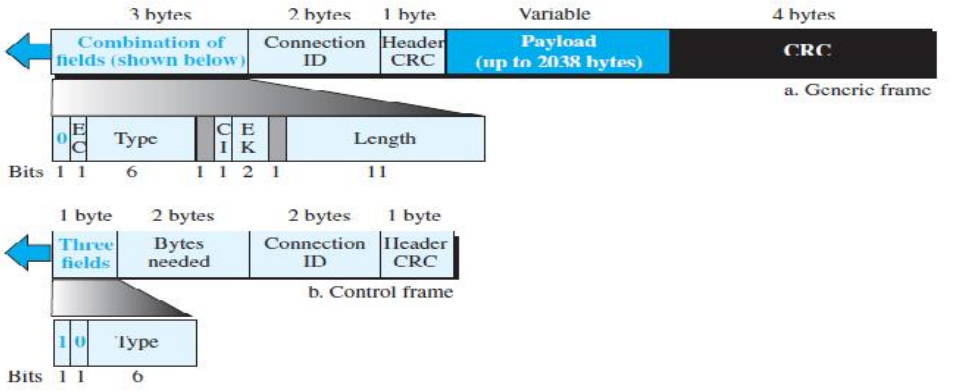
v) Roaming

- Roaming means that a user can have access to communication or can be reached where there is coverage.
- A service provider usually has limited coverage. Neighboring service providers can provide extended coverage through a roaming contract.

8) Explain the Frame format of IEEE 802.16.

- Two types of frames: generic and control.
- The first is used to send and receive payload; the second is used only during the connection establishment. Both frame types use a 6-byte generic header.

Figure 16.4 *WiMAX MAC frame format*



❑ The first bit in a frame is the frame identifier. If it is 0, the frame is a generic frame; if it is 1, it is a control frame.

❑ ***EC.*** The *encryption control* field uses one bit to define whether the frame should be encrypted for security purpose .If the bit is 0, it means no encryption; if it is 1, it means the frame needs to be encrypted at the *security sublayer*,

❑ ***Type.*** The *type* field uses six bits to define the type of the frame. This field is only present in the generic frame and normally is used to define the type of the payload. The payload can be a packed load, a fragmented load

❑ ***CI.*** The *checksum ID* field uses one bit to define whether the frame checksum field should be present or not. If the payload is multimedia, forward error correction is applied (at the physical layer) to the frame and there is no need for checksum.

❑ ***EK.*** The *encryption key* field uses two bits to define one of the four keys for encryption if encryption is required (

❑ ***Length.*** The *length* field uses eleven bits to define the total length of the frame.

❑ ***Bytes Needed.*** The *bytes needed* field uses sixteen bits to define the number of bytes needed for allocated slots in the physical layer.

❑ ***Connection ID.*** The *connection ID* field uses sixteen bits to define the connection identifier for the current connection. Note that the IEEE 802.16 and WiMAX define a connection-oriented protocol, as we discussed before.

❑ ***Header CRC.*** Both types of frames need to have an 8-bit header CRC field. Th eheader CRC is used to check whether the header itself is corrupted. It uses the polynomial $(x^8 + x^2 + x + 1)$ as the divisor.

❑ ***Payload.*** This variable-length field defines the payload, the data that is encapsulated in the frame from the *service specific convergence* sublayer. The field is not needed in the control frame.

❑ ***CRC.*** The last field, if present, is used for error detection over the whole frame. Ituses the same divisor discussed for the Ethernet.