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 ----------

CMR INSTITUTE OF TECHNOLOGY

Scheme Of Evaluation
IMPROVEMENT TEST – May'17

Sub:	DATA COMMUNICATION					**Code:**	15CS46
Date:	29/05/17	Duration:	90mins	Max Marks:	50	**Sem:** IV	**Branch:** ISE

Note: Answer Any Five Question

Question #		Description	Marks Distribution		Max Marks
1	a)	PCF DCF	5M 5M	10M	10 M
2	a)	1-presistent Non-persistent P-persistent	5M	5M	10 M
	b)	Pure ALOHA=$2*T_{fr}$ Slotted ALOHA=T_{fr}	5M	5M	
3	a)	BSSS ,ESSS Picconet and Scatternet	10M	10M	10 M
4		Header format with block diagram	10M	10M	10 M
5		Agents-Home and Foreign Agent 3 phases	3M 7M	10M	10 M
6	a)	Six difference	6M	10M	10 M
	b)	Roaming concept	4M		
7		IFS, Contention window, Acknowledgement Algorithm	10M	10M	10M
8		ICMPV4 about two error messages	10M	10M	10M

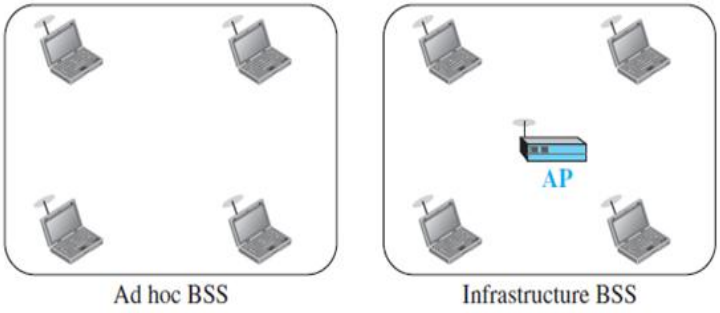
1. Explain the architecture of IEEE 802.11 standards.

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

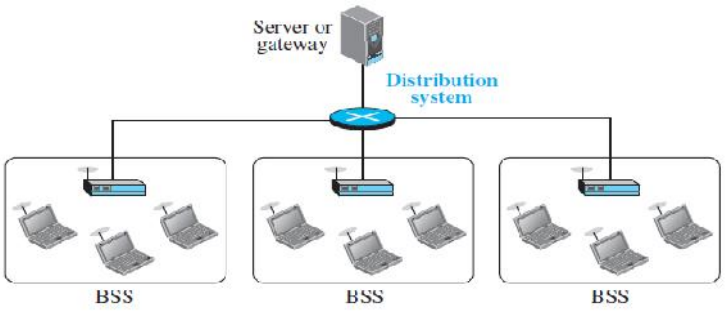
It is made up of two or more BSSs with APs.

- 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.

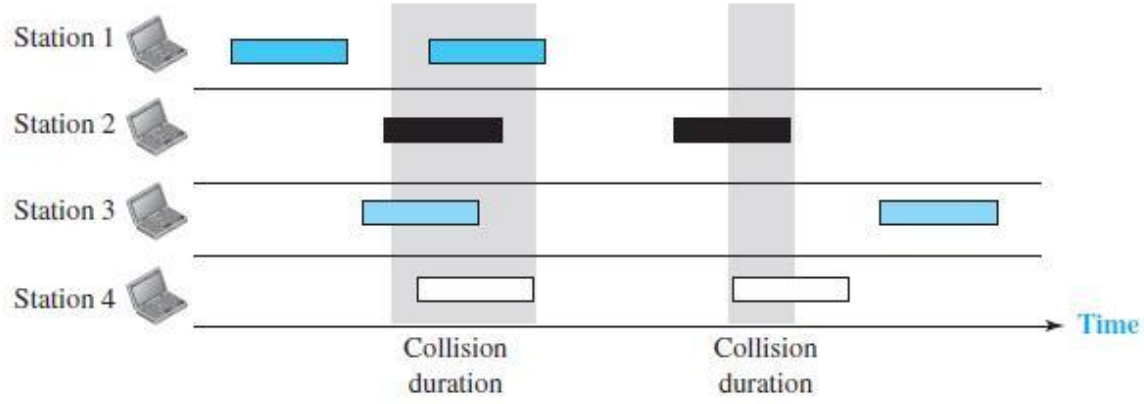
A station with **no-transition mobility** is either stationary (not moving) or moving only inside a BSS.

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.

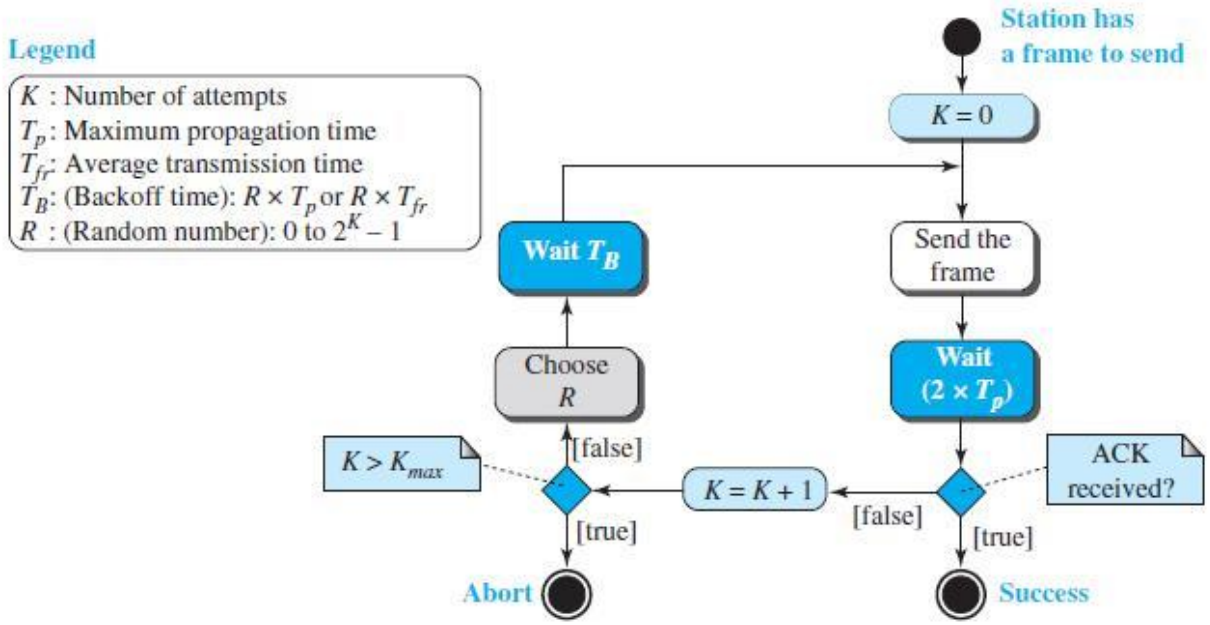
2) ***Pure ALOHA***

The original ALOHA protocol is called ***pure ALOHA.*** The idea is that each station sends a frame whenever it has a frame to send (multiple access). However, since there is only one channel to share, there is the possibility of collision between frames from different stations.



There are four stations (unrealistic assumption) that contend with one another for access to the shared channel. The figure shows that each station sends two frames; there are a total of eight frames on the shared medium. Some of these frames collide because multiple frames are in contention for the shared channel. Figure 12.2 shows that only two frames survive: one frame from station 1 and one frame from station 3. The pure ALOHA protocol relies on acknowledgments from the receiver. When a station sends a frame, it expects the receiver to send an acknowledgment. If the acknowledgment does not arrive after a time-out period, the station assumes that the frame (or the acknowledgment) has been destroyed and resends the frame. A collision involves two or more stations. If all these stations try to resend their frames after the time-out, the frames will collide again. Pure ALOHA dictates that when the time-out period passes, each station waits a random amount of time before resending its frame. The

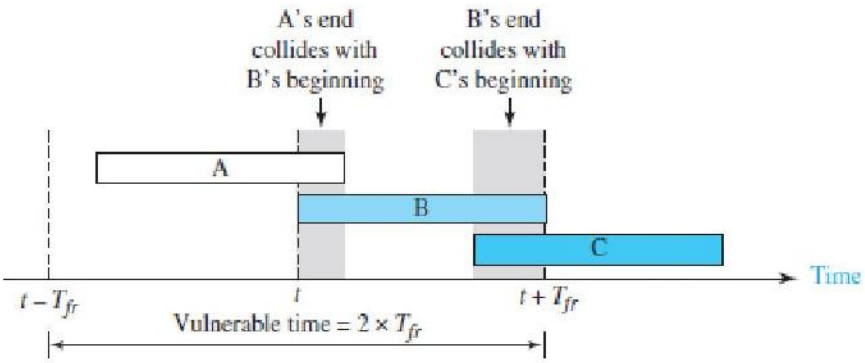
randomness will help avoid more collisions. We call this time the *backoff time TB*. Pure ALOHA has a second method to prevent congesting the channel with retransmitted frames. After a maximum number of retransmission attempts *Kmax*, a station must give up and try later.



Vulnerable time

The ***vulnerable time,*** the length of time in which there is a possibility of collision. We assume that the stations send fixed-length frames with each frame taking *Tfr* seconds to send. Figure 12.4 shows the vulnerable time for station B. Station B starts to send a frame at time *t*. Now imagine station A has started to send its frame after *t* *Tfr*. This leads to a collision between the frames from station B and station A. On the other hand, suppose that station C starts to send a frame before time *t Tfr*. Here, there is also a collision between frames from station B and station C.

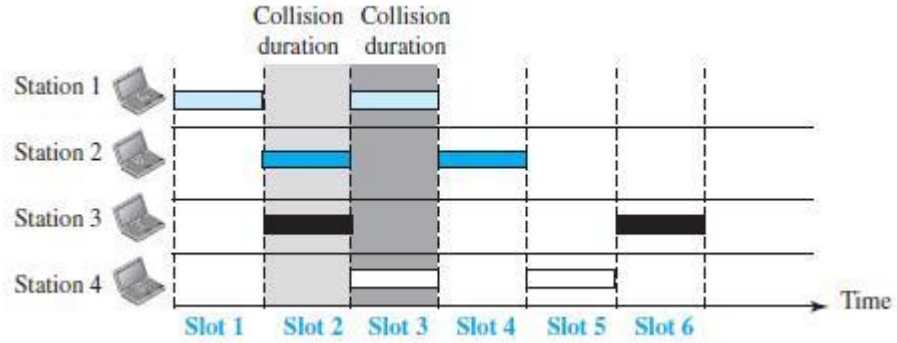
Pure ALOHA vulnerable time = $2 \times T_{fr}$



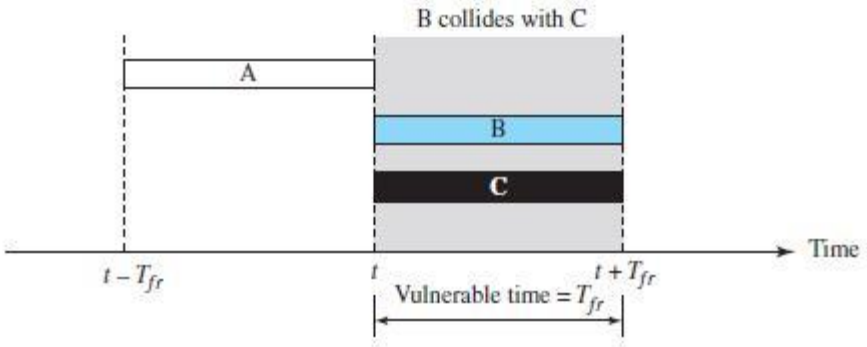
Slotted ALOHA

Pure ALOHA has a vulnerable time of 2 *Tfr*. This is so because there is no rule that defines when the station can send. A station may send soon after another station has started or just before another station has finished. Slotted ALOHA was invented to improve the efficiency of pure ALOHA.

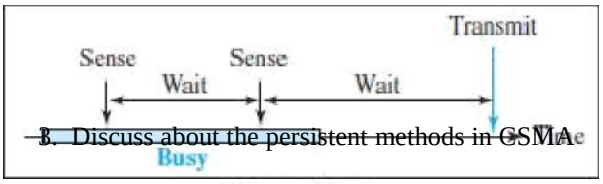
In **slotted ALOHA** we divide the time into slots of *Tfr* seconds and force the station to send only at the beginning of the time slot Because a station is allowed to send only at the beginning of the synchronized time slot, if a station misses this moment, it must wait until the beginning of the next time slot. This means that the station which started at the beginning of this slot has already finished sending its frame. Of course, there is still the possibility of collision if two stations try to send at the beginning of the same time slot. However, the vulnerable time is now reduced to one-half, equal to *Tfr*.



Vulnerable time



Slotted ALOHA vulnerable time = T_{fr}

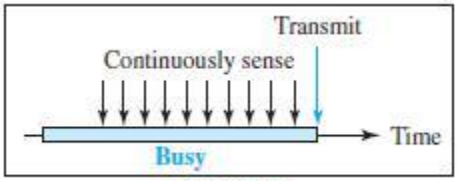


b. Nonpersistent

3. Discuss about the persistent methods in CSMA/CA

Persistence Methods 1-Persistent

The *1-persistent method* is simple and straightforward. In this method, after the station finds the line idle, it sends its frame immediately (with probability 1). This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.



a. 1-Persistent

Nonpersistent

In the *nonpersistent method*, a station that has a frame to send senses the line. If the line is idle, it sends immediately. If the line is not idle, it waits a random amount of time and then senses the line again. The nonpersistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously. However, this method reduces the efficiency of the network because the medium remains idle when there may be stations with frames to send.

p-*Persistent*

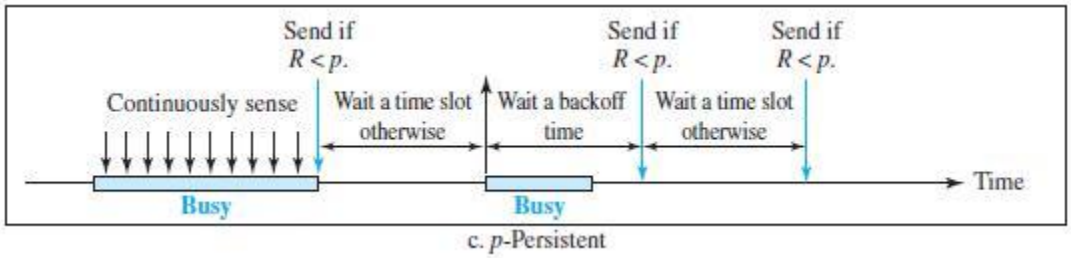
The p-*persistent method* is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time. The *p*-persistent approach combines the advantages of the other two strategies. It reduces the chance of collision and improves efficiency. In this method, after the station finds the line idle it follows these steps:

1. With probability *p*, the station sends its frame.

2. With probability *q* 1 *p*, the station waits for the beginning of the next time slot and checks the line again.

a. If the line is idle, it goes to step 1.

b. If the line is busy, it acts as though a collision has occurred and uses the backoff procedure.



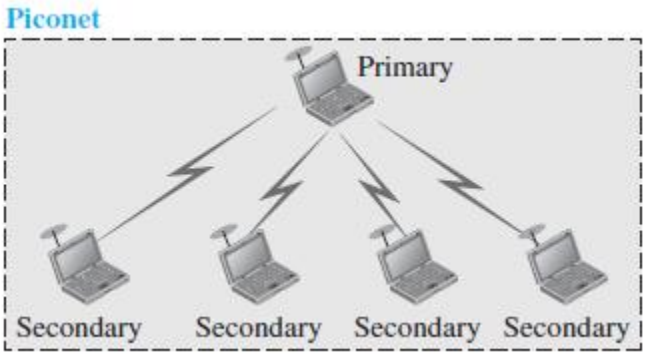
c. *p*-Persistent

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.

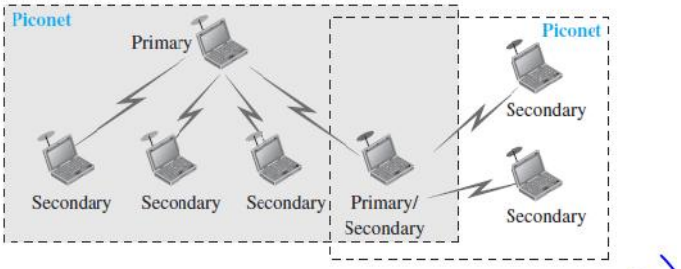


- Although a piconet can have a maximum of seven secondaries, additional secondaries can be in the *parked state*.
- A secondary in a parked state is synchronized with the primary, but cannot take part in communication until it is moved from the parked state to the active state. Because only eight stations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

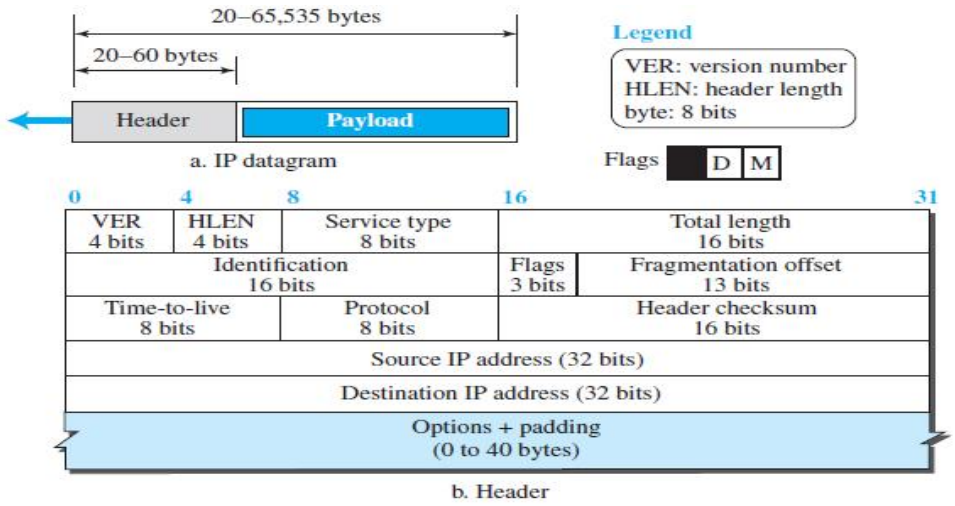
ii) Scatternet

- 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.

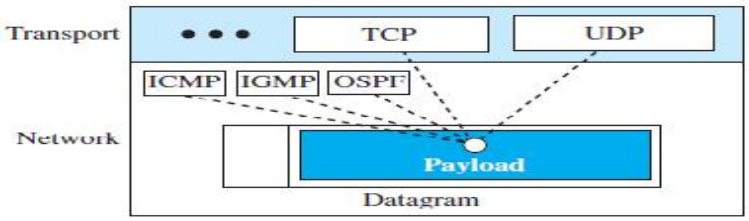
Time-to-live.

- 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.

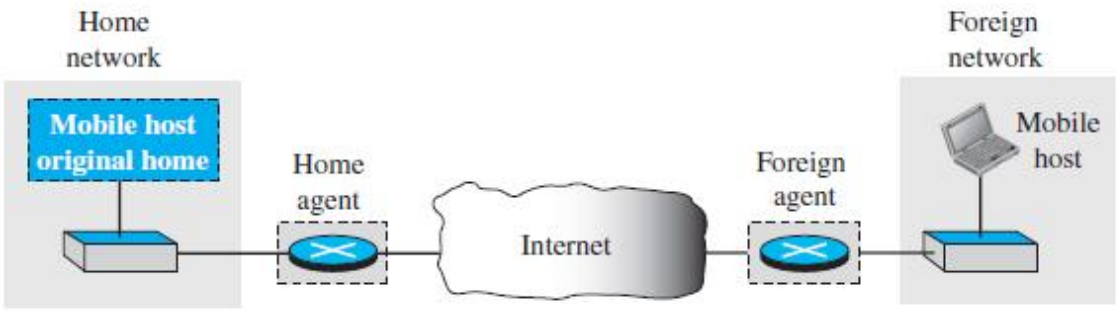
- Payload, or data, is the main reason for creating a datagram.
- Payload is the packet coming from other protocols that use the service of IP.

5) What is Agents in Mobile IP? Explain three phases in it

Agents

To make the change of address transparent to the rest of the Internet requires a **home agent** and a **foreign agent.**

Figure 19.13 *Home agent and foreign agent*



Home Agent

The home agent is usually a router attached to the home network of the mobile host. The home agent acts on behalf of the mobile host when a remote host sends a packet to the mobile host. The home agent receives the packet and sends it to the foreign agent.

Foreign Agent

The foreign agent is usually a router attached to the foreign network. The foreign agent receives and delivers packets sent by the home agent to the mobile host. The mobile host can also act as a foreign agent. In other words, the mobile host and the foreign agent can be the same. When the mobile host acts as a foreign agent, the care-of address is called a **collocated care-of address.**

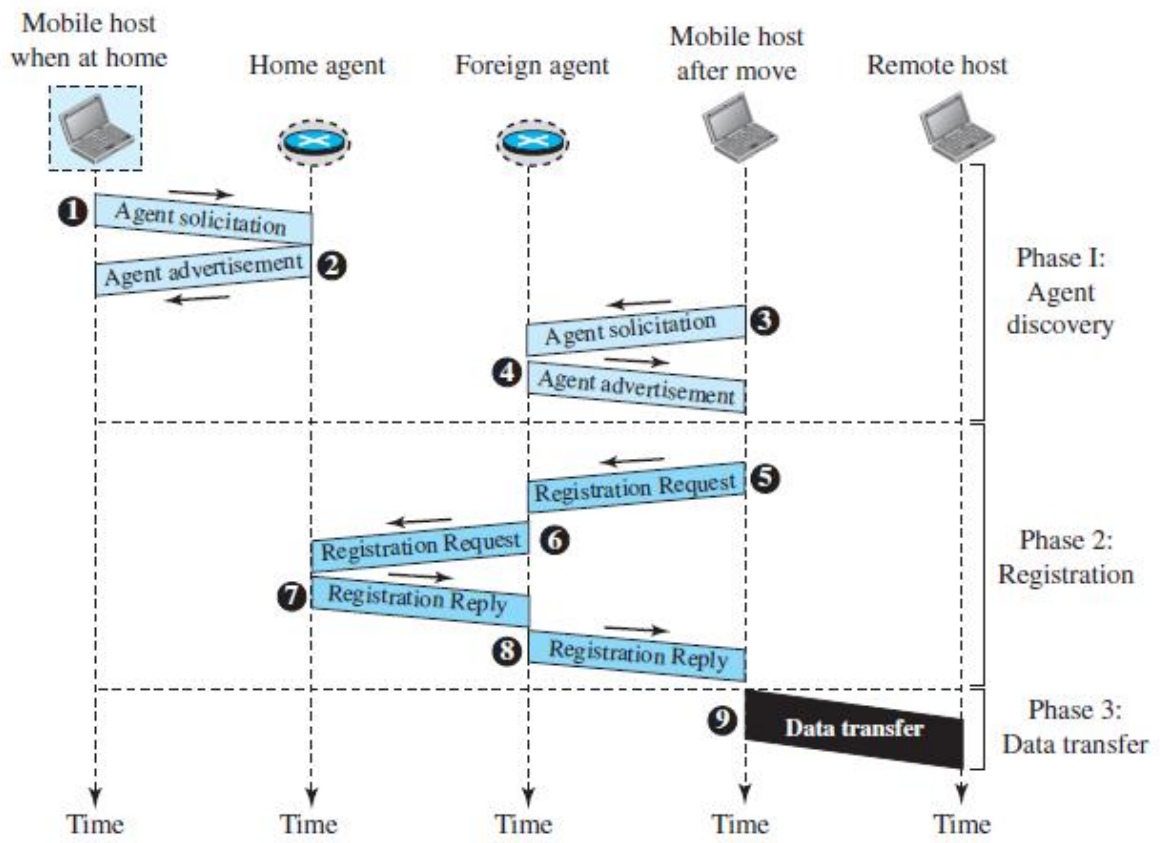
The advantage of using a collocated care-of address is that the mobile host can move to any network without worrying about the availability of a foreign agent.

The disadvantage is that the mobile host needs extra software to act as its own foreign agent.

Three Phases

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

The first phase, agent discovery, involves the mobile host, the foreign agent, and the home agent. The second phase, registration, also involves the mobile host and the two agents. Finally, in the third phase, the remote host is also involved.



Agent Discovery

The first phase in mobile communication, *agent discovery*, consists of two subphases. 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.

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.

ICMP Advertisement message			
Type	Length	Sequence number	
Lifetime		Code	Reserved
Care-of addresses (foreign agent only)			

Agent Solicitation

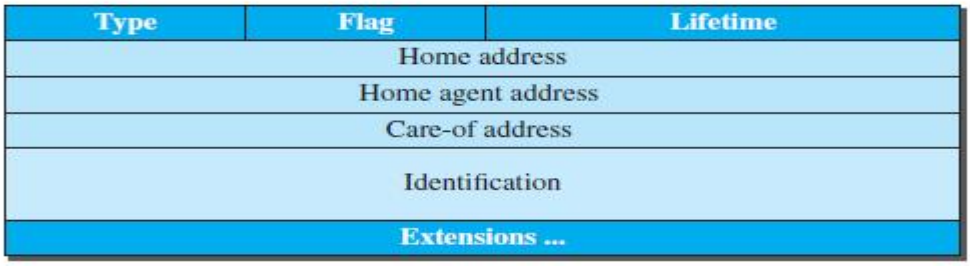
When a mobile host has moved to a new network and has not received agent advertisements,it can initiate an *agent solicitation.* It can use the ICMP solicitation message to inform an agent that it needs assistance.

Registration

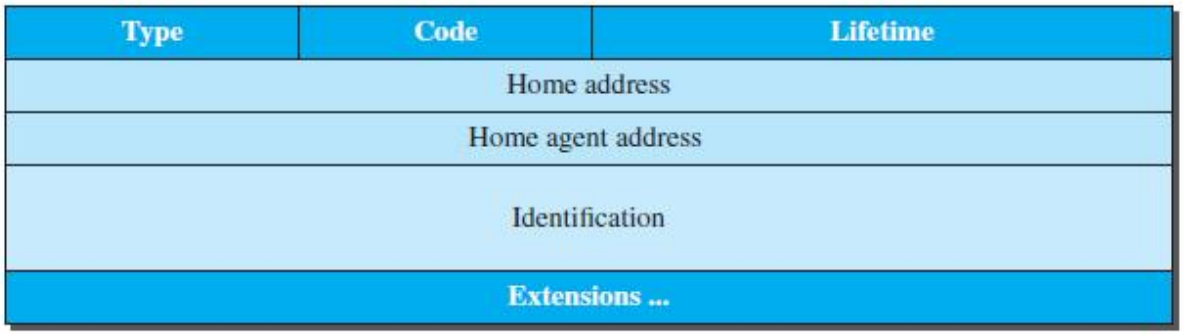
The second phase in mobile communication is *registration.* After a mobile host has moved to a foreign network and discovered the foreign agent, it must register. There are four aspects of registration:

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.

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.



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.



Data Transfer

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

From Remote Host to Home Agent

When a remote host wants to send a packet to the mobile host, it uses its address as the source address and the home address of the mobile host as the destination address.

From Home Agent to Foreign Agent

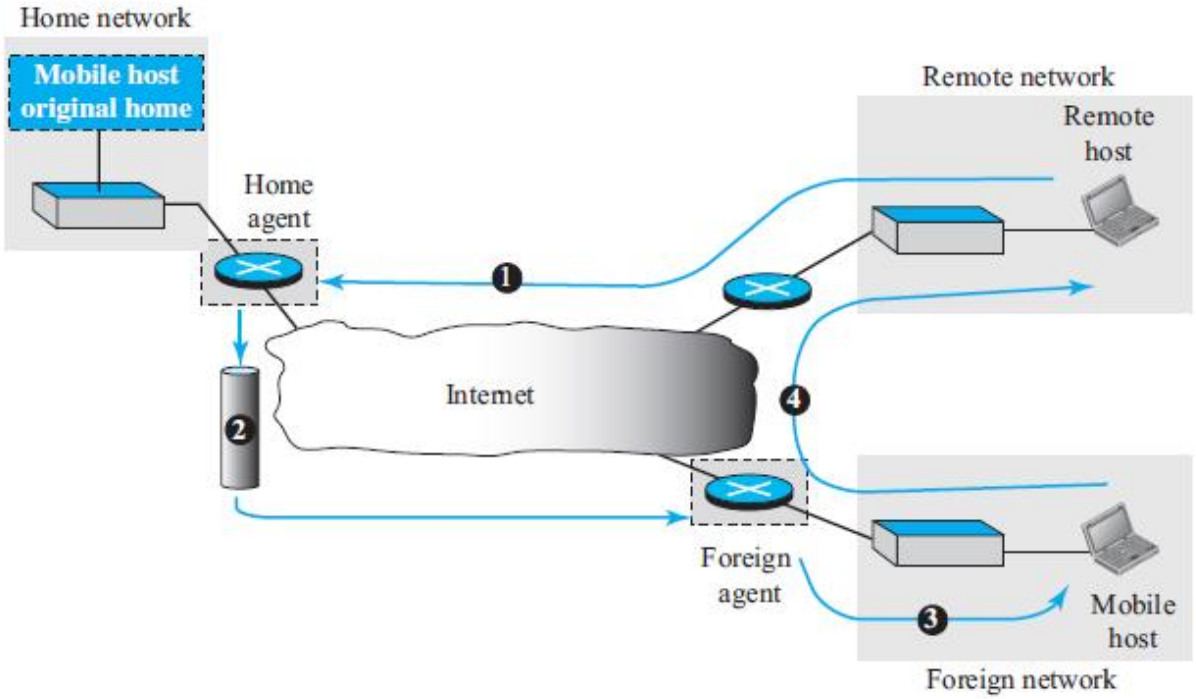
After receiving the packet, the home agent sends the packet to the foreign agent.

From Foreign Agent to Mobile Host

When the foreign agent receives the packet, it removes the original packet. However, since the destination address is the home address of the mobile host, the foreign agent consults a registry table to find the care-of address of the mobile host.

From Mobile Host to Remote Host

When a mobile host wants to send a packet to a remote host (for example, a response to the packet it has received), it sends as it does normally. The mobile host prepares apacket with its home address as the source, and the address of the remote host as the destination.

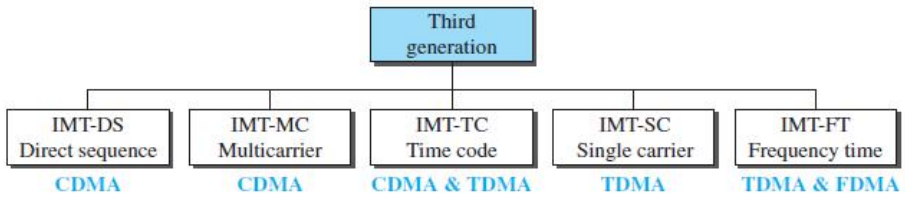


6a) Write short note on 3G systems

- 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) ***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.

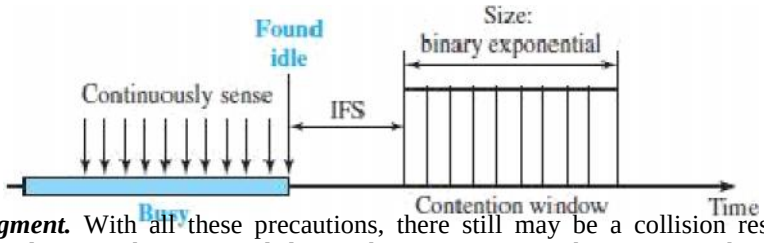
7) Explain in detail about CSMA/CA

Carrier sense multiple access with collision avoidance (CSMA/CA) was invented for wireless networks.

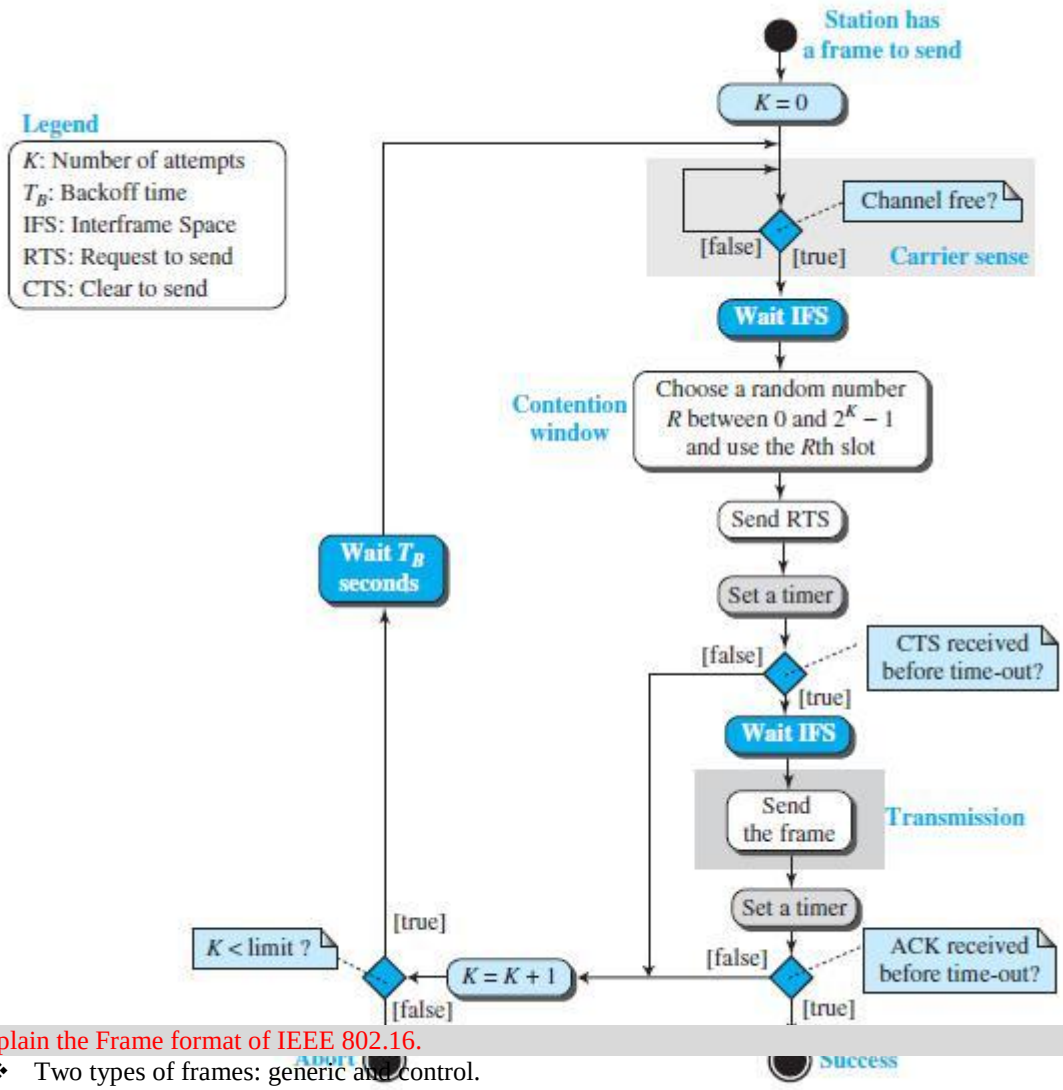
Collisions are avoided through the use of CSMA/CA's three strategies: the interframe space, the contention window, and acknowledgments .

Interframe Space (IFS). First, 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 ***interframe space*** or ***IFS.*** Even though the channel may appear idle when it is sensed, a distant station may have already started transmitting. The distant station's signal has not yet reached this The IFS time allows the front of the transmitted signal by the distant station to reach this station. After waiting an IFS time, if the channel is still idle, the station can send, but it still needs to wait a time equal to the contention window.

Contention Window. The **contention window** is an amount of time divided into slots. A station that is ready to send chooses a random number of slots as its wait time. The number of slots in the window changes according to the binary exponential backoff strategy. This means that it is set to one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time. This is very similar to the *p*-persistent method except that a random outcome defines the number of slots taken by the waiting station.



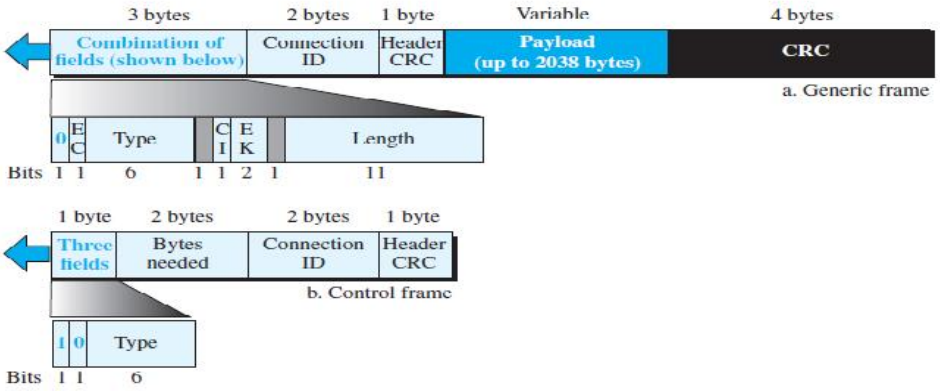
Acknowledgment. With all these precautions, there still may be a collision resulting in destroyed data. In addition, the data may be corrupted during the transmission. The positive acknowledgment and the time-out timer can help guarantee that the receiver has received the frame.



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 ($x8 \quad x2 \quad x \quad 1$) 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.