December 2010

Q.1.A) What is the reason for a handoff in cellular networks?Explain the various types of handoffs and the stratergies used for handoff.

Ans) 1. Cellular systems require handover procedures, as single cells do not cover the whole service area, but eg. Only up to 35 km around each antenna on the countryside and some hundred meters in cities.
2. The smaller the cell size and the faster the movement of the mobile station through the cells (up to 250 km/h for GSM) the more handovers of ongoing calls are required. However handover should not cause cut-off called as call drop.
3. GSM aims at maximum handover duration of 60 ms.

4. There two basic reasons for handover those are:

A. The mobile station moves out of the range of a BTS or a certain antenna of a BTS respectively. The received signal level decreases continuously until it falls below the minimal requirements for communication. The error rate may grow due to interference, the distance to the BTS may to high (max. 35 km) etc. – all these effects may diminish the quality of the radio link and make radio transmission impossible in the near future.

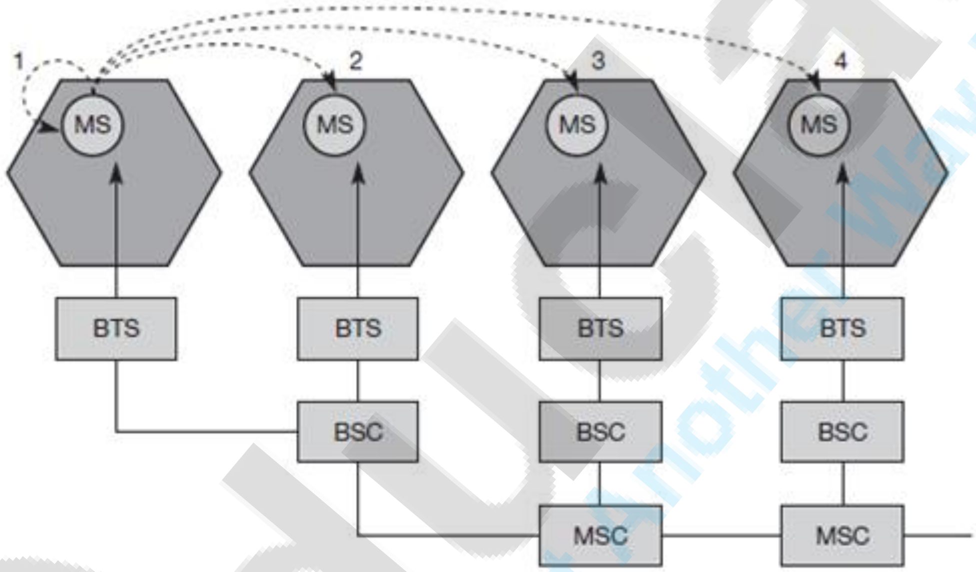
B. The wired infrastructure (MSC, BSC) may decide that the traffic in one cell is too high and shift some MS to other cells with a lower load (if possible). Handover may be due to load balancing.

5. Possible handover scenarios in GSM:

A. Intra-cell handover: within a cell, narrow band interference could make transmission at a certain frequency impossible. The BSC then could decide to change the carrier frequency.
B. Inter-cell, intra-BSC handover: this is a typical handover scenario. The mobile station moves from one cell to another, but stays within the control of the same BSC. The BSC then performs a handover, assigns a new radio channel in the new cell and releases the old one.
C. Inter-BSC, intra-MSC handover: as a BSC only controls the limited number of cells; GSM also has to perform handover between cells controlled by different BSCs. This handover then has to be controlled by the MSC.
D. Inter MSC handover: a handover could be required between two cells belonging to different MSCs. Now both MSCs perform the handover together.

6. To provide all the necessary information for a handover due to a weak link, MS and BTS both perform periodic measurements of the downlink and uplink quality respectively.

7. Link quality consists of signal level and bit error rate. Measurement reports are sent by the MS about every half second and contain the quality of the current link used for transmission as well as the quality of the certain channels in neighbouring cells (the BCCHs).
8. More sophisticated handover mechanisms are needed for seamless handovers between different systems. For example, future 3G networks will not cover whole countries but focus on the cities and highways.
9. Handover from eg., UMTS to GSM without service interruption must be possible. Even more challenging is the seamless handover between wireless LANs and 2G/3G networks. This can be done using multimode mobile stations and a more sophisticated roaming infrastructure.
10. Following figure shows the different types of handovers in GSM system:



Q.1.B)Discuss the various modulation techniques used in the wireless transmissions.

Ans: In wireless networks, the binary bit-stream has to be translated into an analog signal first. The three basic methods for this translation are amplitude shift keying (ASK), frequency shift keying (FSK), and phase shift keying (PSK). Apart from the translation of digital data into analog signals, wireless transmission requires an additional modulation, an analog modulation that shifts the center frequency of the baseband signal generated by the digital modulation up to the radio carrier. For example, digital modulation translates a 1 Mbit/s bit-stream into a baseband signal with a bandwidth of 1 MHz.

<u>Amplitude shift keying:</u>
Figure (1) illustrates amplitude shift keying (ASK), the most simple digital modulation scheme.

The two binary values, 1 and 0, are represented by two different amplitudes. In the example, one of the amplitudes is 0 (representing the binary 0). This simple scheme only requires low bandwidth, but is very susceptible to interference. Effects like multi-path propagation, noise, or path loss heavily influence the amplitude. In a wireless environment, a constant amplitude cannot be guaranteed, so ASK is typically not used for wireless radio transmission. However, the wired transmission scheme with the highest performance, namely optical transmission, uses ASK. Here, a light pulse may represent a 1, while the absence of light represents a 0. The carrier frequency in optical systems is some hundred THz. ASK can also be applied to wireless infrared transmission, using a directed beam or diffuse light.

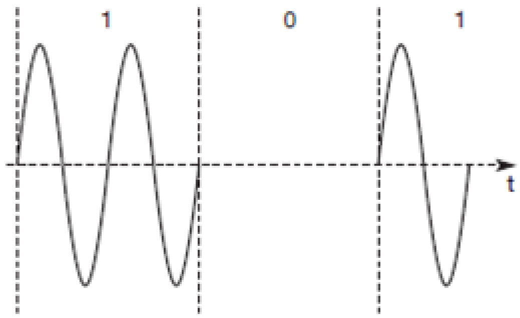


Figure 1. Amplitude shift keying (ASK)

Frequency shift keying:

A modulation scheme often used for wireless transmission is frequency shift keying (FSK). The simplest form of FSK, also called binary FSK (BFSK), assigns one frequency f1 to the binary 1 and another frequency f2 to the binary 0. A very simple way to implement FSK is to switch between two oscillators, one with the frequency f1 and the other with f2, depending on the input. To avoid sudden changes in phase, special frequency modulators with continuous phase modulation (CPM) can be used. Sudden changes in phase cause high frequencies, which is anundesired side-effect.A simple way to implement demodulation is by using two band pass filters, one for f1 the otherfor f2. A comparator can then compare the signal levels of the filter outputs to decide which of them is stronger. FSK needs a larger bandwidth compared to ASK but is much less susceptible to errors.

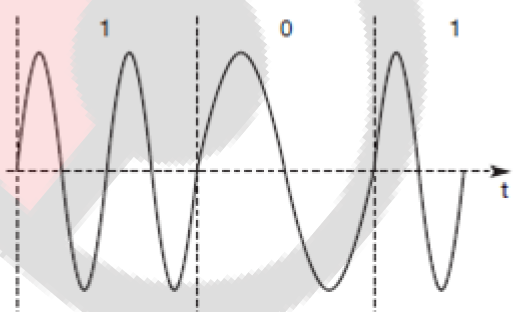


Figure 2. Frequency shift keying (FSK)

Phase shift keying:

Phase shift keying (PSK) uses shifts in the phase of a signal to represent data. Figure (3) shows a phase shift of 180° or π as the 0 follows the 1 (the same happens as the 1 follows the 0). This simple scheme, shifting the phase by 180° each time the value of data changes, is also called binary PSK (BPSK). A simple implementation of a BPSK modulator could multiply a frequency f with +1 if the binary data is 1 and with –1 if the binary data is 0.
To receive the signal correctly, the receiver must synchronize in frequency and phase with the transmitter. This can be done using a phase lock loop (PLL).
Compared to FSK, PSK is more resistant to interference, but receiver and transmitter are also more complex.

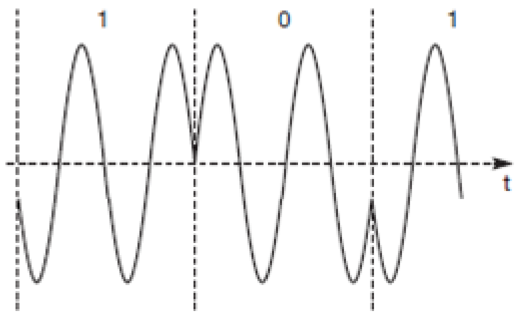


Figure 3. Phase shift keying (PSK)

Q.2

a) What are the J2ME configurations and profiles?

The configuration defines the basic run-time environment as a set of core classes and a specific JVM that run on specific types of devices. You also learned that the two types of configurations for J2ME are CLDC and CDC.
A J2ME environment can be configured dynamically to provide the environment needed to run an application, regardless of whether or not all Java technology-based libraries necessary to run the application are present on the device. The core platform receives both application code and libraries. Configuration is performed by server software running on the network.

Connected Limited Device Configuration (CLDC)

CLDC was created by the Java Community Process, which has standardized this "portable, minimum-footprint Java building block for small, resource-constrained devices," as defined on Sun Microsystems' Web site.

The J2ME CLDC configuration provides for a virtual machine and set of core libraries to be used within an industry-defined profile. A profile defines the applications for particular devices by supplying domain-specific classes on top of the base J2ME configuration. The K virtual machine

(KVM), CLDC's reference implementation of a virtual machine, and its KJava profile run on top of CLDC.

CLDC outlines the most basic set of libraries and Java virtual machine features required for each implementation of J2ME on highly constrained devices. CLDC targets devices with slow network connections, limited power (often battery operated), 128 KB or more of non-volatile memory, and 32 KB or more of volatile memory. Volatile memory is non-persistent and has no write protection, meaning if the device is turned off, the contents of volatile memory are lost. With non-volatile memory, contents are persistent and write protected. CLDC devices use non-volatile memory to store the run-time libraries and KVM, or another virtual machine created for a particular device. Volatile memory is used for allocating run-time memory.

CLDC requirements

- Full Java language support (except for floating pointer support, finalization, and error handling)
- Full JVM support
- Security for CLDC
- Limited internationalization support
- Inherited classes -- all classes not specific to CLDC must be subsets of J2SE 1.3
- Classes specific to CLDC are in javax.microedition package and subpackages.

In addition to the javax.microedition package, the CLDC API consists of subsets of the J2SE java.io, java.lang, and java.util packages. We will cover details in the section on CLDC API on page 18and will use the CLDC API to develop our drawing application.

Connected Device Configuration (CDC)

Connected Device Configuration (CDC) has been defined as a stripped-down version of Java 2 Standard Edition (J2SE) with the CLDC classes added to it. Therefore, CDC was built upon CLDC, and as such, applications developed for CLDC devices also run on CDC devices. CDC, also developed by the Java Community Process, provides a standardized, portable, full-featured Java 2 virtual machine building block for consumer electronic and embedded devices, such as smartphones, two-way pagers, PDAs, home appliances, point-of-sale terminals, and car navigation systems. These devices run a 32-bit microprocessor and have more than 2 MB of memory, which is needed to store the C virtual machine and libraries. While the K virtual machine supports CLDC, the C virtual machine (CVM) supports CDC.

What is a J2ME profile?

The Mobile Information Device Profile (MIDP), for example, defines classes for cellular phones. It adds domain-specific classes to the J2ME configuration to define uses for similar devices. Two profiles have been defined for J2ME and are built upon CLDC: KJava and MIDP. Both KJava and MIDP are associated with CLDC and smaller devices. Profiles are built on top of

configurations. Because profiles are specific to the size of the device (amount of memory) on which an application runs, certain profiles are associated with certain configurations.
A skeleton profile upon which you can create your own profile, the Foundation Profile, is available for CDC. However, for this tutorial and this section, we will focus only on the KJava and MIDP profiles built on top of CLDC.

Profile 1: **KJava**
KJava is Sun's proprietary profile and contains the KJava API. The KJava profile is built on top of the CLDC configuration. The KJava virtual machine, KVM, accepts the same byte codes and class file format as the classic J2SE virtual machine.
KJava contains a Sun-specific API that runs on the Palm OS. The KJava API has a great deal in common with the J2SE Abstract Windowing Toolkit (AWT). However, because it is not a standard J2ME package, its main package is com.sun.kjava. We'll learn more about the KJava API later in this tutorial when we develop some sample applications.

Profile 2: **MIDP**
MIDP is geared toward mobile devices such as cellular phones and pagers. The MIDP, like KJava, is built upon CLDC and provides a standard run-time environment that allows new applications and services to be deployed dynamically on end-user devices.
MIDP is a common, industry-standard profile for mobile devices that is not dependent on a specific vendor. It is a complete and supported foundation for mobile application development. MIDP contains the following packages, the first three of which are core CLDC packages, plus three MIDP-specific packages. We will discuss each of these packages later on in the tutorial:

* java.lang
* java.io
* java.util
* javax.microedition.io
* javax.microedition.lcdui
* javax.microedition.midlet

b) What is CDMA?

CDMA (Code-Division Multiple Access) is a channel access method used by various radio communication technologies. It is a form of multiplexing, which allows numerous signals to occupy a single transmission channel, optimizing the use of available bandwidth. The technology is used in ultra-high-frequency (UHF) cellular telephone systems in the 800-MHz and 1.9-GHz bands.

CDMA employs analog-to-digital conversion (ADC) in combination with spread spectrum technology. Audio input is first digitized into binary elements. The frequency of the transmitted signal is then made to vary according to a defined pattern (code), so it can be intercepted only by a receiver whose frequency response is programmed with the same code, so it follows exactly along with the transmitter frequency. There are trillions of possible frequency-sequencing codes, which enhances privacy and makes cloning difficult.

<u>Key elements of CDMA</u>
CDMA is a form of spread spectrum transmission technology. It has a number of distinguishing features that are key to spread spectrum transmission technologies:

- *Use of wide bandwidth:* CDMA, like other spread spectrum technologies uses a wider bandwidth than would otherwise be needed for the transmission of the data. This results in a number of advantages including an increased immunity to interference or jamming, and multiple user access.
- *Spreading codes used:* In order to achieve the increased bandwidth, the data is spread by use of a code which is independent of the data.
- *Level of security:* In order to receive the data, the receiver must have a knowledge of the spreading code, without this it is not possible to decipher the transmitted data, and this gives a measure of security.
- *Multiple access:* The use of the spreading codes which are independent for each user along with synchronous reception allow multiple users to access the same channel simultaneously.

Advantages of CDMA techniques:

Ø Efficient practical utilization of fixed frequency spectrum.
Ø Flexible allocation of resources.
Ø Many users of CDMA use the same frequency, TDD or FDD may be used
Ø Multipath fading may be substantially reduced because of large signal bandwidth
Ø No absolute limit on the number of users, Easy addition of more users.
Ø Impossible for hackers to decipher the code sent
Ø Better signal quality
Ø No sense of handoff when changing cells
Ø The CDMA channel is nominally 1.23 MHz wide.

Ø CDMA networks use a scheme called soft handoff, which minimizes signal breakup as a handset passes from one cell to another.
Ø CDMA is compatible with other cellular technologies; this allows for nationwide roaming.
Ø The combination of digital and spread-spectrum modes supports several times as many signals per unit bandwidth as analog modes.

Disadvantages to using CDMA:

Ø As the number of users increases, the overall quality of service decreases
Ø Self-jamming
Ø Near- Far- problem arises

Uses of CDMA:
Ø One of the early applications for code division multiplexing is in GPS. This predates and is distinct from its use in mobile phones.
Ø The Qualcomm standard IS-95, marketed as cdmaOne.
Ø The Qualcomm standard IS-2000, known as CDMA2000. This standard is used by several mobile phone companies, including the Globalstar satellite phone network.
Ø The UMTS 3G mobile phone standard, which uses W-CDMA.
Ø CDMA has been used in the OmniTRACS satellite system for transportation logistics.

CDMA vs WCDMA

1.CDMA is a 2G technology while WCDMA is a 3G technology
2. CDMA and WCDMA are not used together
3. WCDMA offers much faster speeds compared to CDMA
4. CDMA uses frequency bands 1.25Mhz wide while WCDMA uses frequency bands 5Mhz wide
5. The WCDMA doesn’t share the same design as CDMA
6. CDMA and its successors are being phased out in favor of GSM and WCDMA

Q 3 (a) Explain the various states that a Bluetooth enabled device can move into.
Ans:
Bluetooth supports both point-to-point and point-to- multi-point connections. Several piconets can be established and linked together ad hoc, where each piconet is identified by a different frequency hopping sequence. All users participating on the same piconet are synchronized to this hopping sequence.

The following are the states of a bluetooth device:
Stand-by mode:

Before any connections in a piconet are created, all devices are in STANDBY mode. In this mode, an unconnected unit periodically "listens" for messages every 1.28 seconds.
Each time a device wakes up, it listens on a set of 32 hop frequencies defined for that unit.
The connection procedure is initiated by any of the devices that then becomes master.

Page and Inquiry State:

A connection is made by a PAGE message if the address is already known, or by an INQUIRY message followed by a subsequent PAGE message if the address is unknown.
In the initial PAGE state, the master unit will send a train of 16 identical page messages on 16 different hop frequencies defined for the device to be paged (slave unit). If no response, the master transmits a train on the remaining 16 hop frequencies in the wake-up sequence.
The INQUIRY message is typically used for finding Bluetooth devices with an unknown address, it is very similar to the page message, but may require one additional train period to collect all the responses.

Connection Modes

Devices synchronized to a piconet can enter power-saving modes in which device activity is lowered. A Bluetooth device in the *Connection* state can be in any of the four following modes:

Active Mode:

In the active mode, the Bluetooth unit actively participates on the channel. The master schedules the transmission based on traffic demands to and from the different slaves.
It supports regular transmissions to keep slaves synchronized to the channel.
Active slaves listen in the master-to-slave slots for packets and if an active slave is not addressed, it may sleep until the next new master transmission.

Sniff Mode:

In the SNIFF mode, a slave device listens to the piconet at reduced rate, thus reducing its duty cycle.
The SNIFF interval is programmable and depends on the application.
It has the highest duty cycle (least power efficient) of all 3 power saving modes (sniff, hold & park).

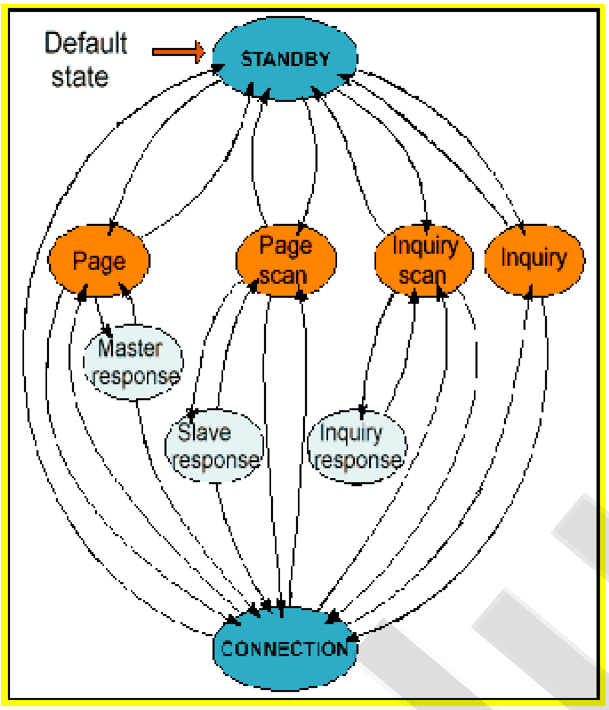
Hold Mode:

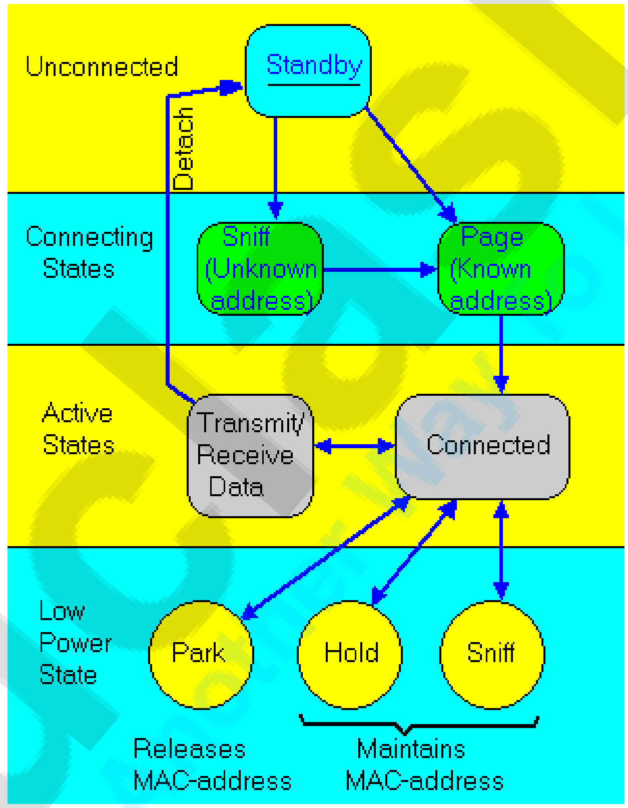
The master unit can put slave units into HOLD mode, where only an internal timer is running.
Slave units can also demand to be put into HOLD mode.
Data transfer restarts instantly when units transition out of HOLD mode.
It has an intermediate duty cycle (medium power efficient) of the 3 power saving modes (sniff, hold & park).

Park Mode:

In the PARK mode, a device is still synchronized to the piconet but does not participate in the traffic.
Parked devices have given up their MAC (AM_ADDR) address and occasional listen to the traffic of the master to re-synchronize and check on broadcast messages.
It has the lowest duty cycle (power efficiency) of all 3 power saving modes (sniff, hold & park).

The following is a graphical illustration of the above mentioned states:





Q-4

a)What is fading? Explain the type of fading .how does the fading effect the wireless transmission?

Ans-> fading is deviation of the attenuation that a carrier-modulated telecommunication signal experiences over certain propagation media. The fading may vary with time, geographical position and/or radio frequency, and is often modelled as a random process. A fading channel is a communication channel that experiences fading. In wireless systems, fading may either be due to multipath propagation, referred to as multipath induced fading, or due to shadowing from obstacles affecting the wave propagation, sometimes referred to as shadow fading

Key concepts

The presence of reflectors in the environment surrounding a transmitter and receiver create multiple paths that a transmitted signal can traverse. As a result, the receiver sees the superposition of multiple copies of the transmitted signal, each traversing a different path. Each signal copy will experience differences in attenuation, delayand phase shift while travelling from the source to the receiver. This can result in either constructive or destructive interference, amplifying or attenuating the signal power seen at the receiver. Strong destructive interference is frequently referred to as a deep fade and may result in temporary failure of communication due to a severe drop in the channel signal-to-noise ratio.

A common example of multipath fading is the experience of stopping at a traffic light and hearing an FM broadcast degenerate into static, while the signal is re-acquired if the vehicle moves only a fraction of a meter. The loss of the broadcast is caused by the vehicle stopping at a point where the signal experienced severe destructive interference. Cellular phones can also exhibit similar momentary fades.

Fading channel models are often used to model the effects of electromagnetic transmission of information over the air in cellular networks and broadcast communication. Fading channel models are also used in underwater acoustic communications to model the distortion caused by the water. Mathematically, fading is usually modeled as a time-varying random change in the amplitude andphase of the transmitted signal.

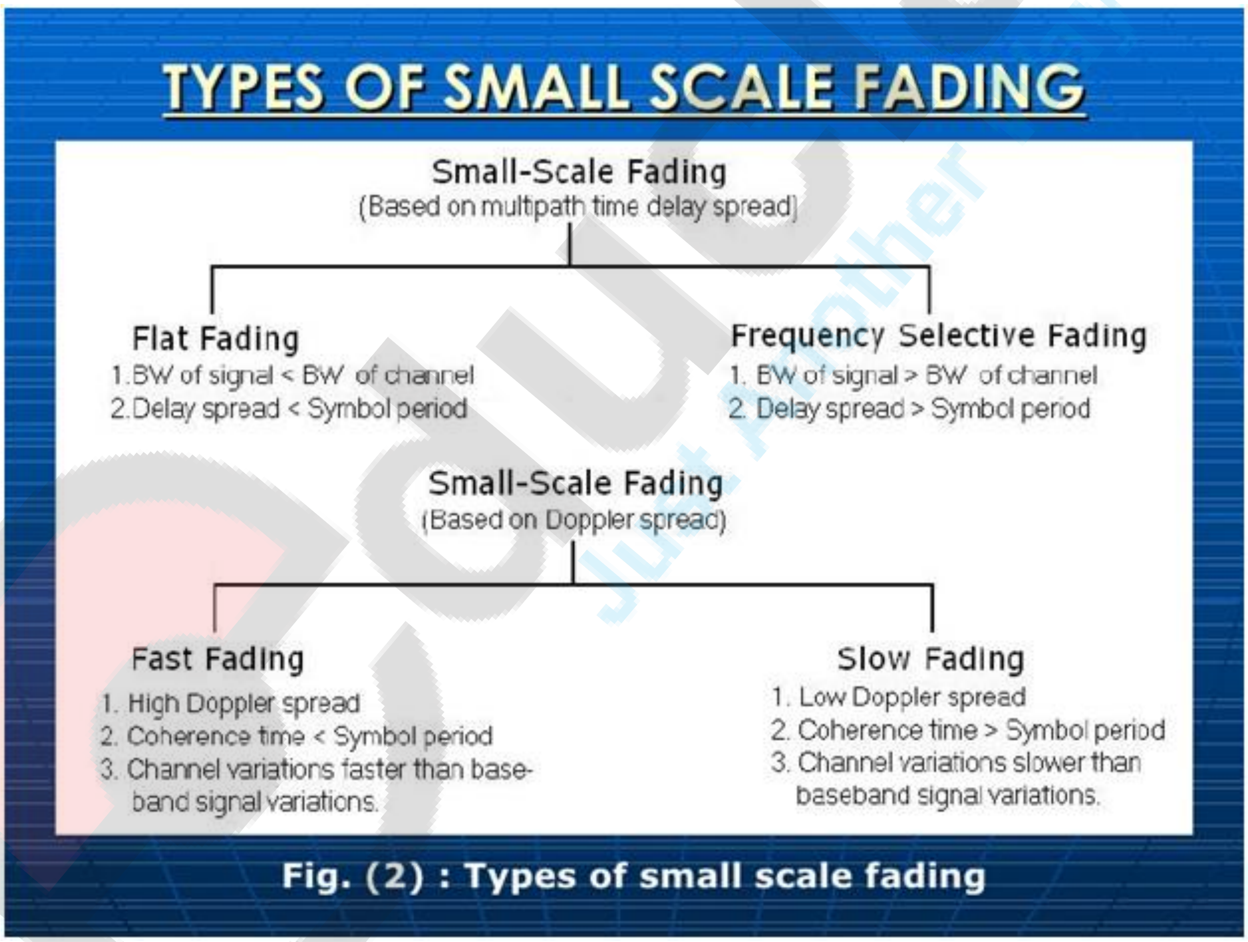
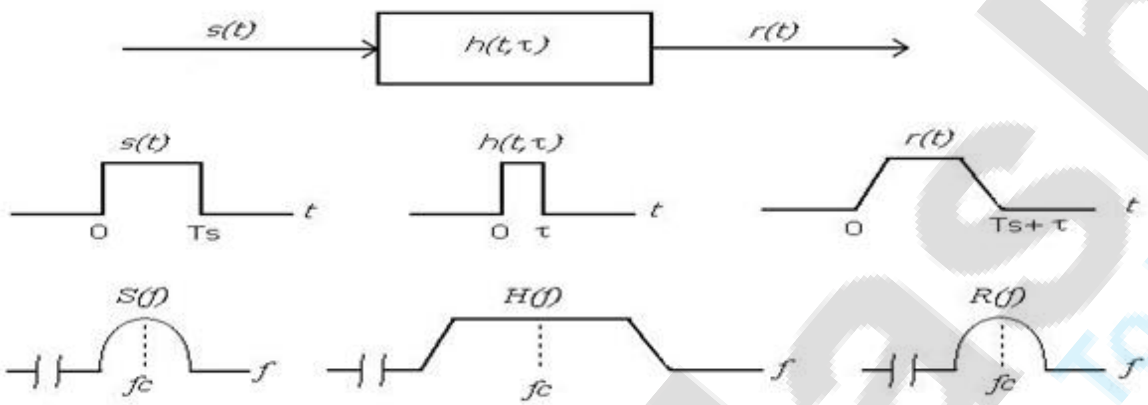


Fig. (2) : Types of small scale fading

FLAT FADING:-

Flat fading, where the bandwidth of the signal is less than the coherence bandwidth of the channel or the delay spread is less than the symbol period.



<u>FREQUENCY SELECTIVE FADING:-></u>

Frequency selective fading, where the bandwidth of the signal is greater than the coherence bandwidth of the channel or the delay spread is greater than the symbol period.

<u>FAST FADING:-></u>

Fast Fading is a kind of fading occurring with small movements of a mobile or obstacle.

Depending upon how rapidly the transmitted base band signal changes as compared to the rate of change of the channel.

The channel may be classified either as a Flat fading or Slow fading channel.

In a Fast fading channel, the impulse response changes rapidly within the symbol duration. That is, the coherence time of the channel is smaller than the symbol period of the transmitted signal. This causes frequency dispersion (also called the selective fading) due to Doppler spreading, which leads to signal distortion.

<u>SLOW FADING:-></u>

Slow Fading is a kind of fading caused by larger movements of a mobile or obstructions within the propagation environment. This is often modeled as log-normal distribution with a standard deviation according to the Log Distance Path Loss Model.

In a slow fading channel, the channel impulse response changes at a rate much slower than the transmitted base band signal s(t). In this case, channel may be assumed to be static over one or several reciprocal bandwidth intervals.

Multipath Fading Effects

1. Rapid changes in signal strength over a small travel distance or time interval.
2. Random frequency modulation due to varying Doppler shifts on different mul-

tipath signals.
Time dispersion or echoes caused by multipath propagation delays.

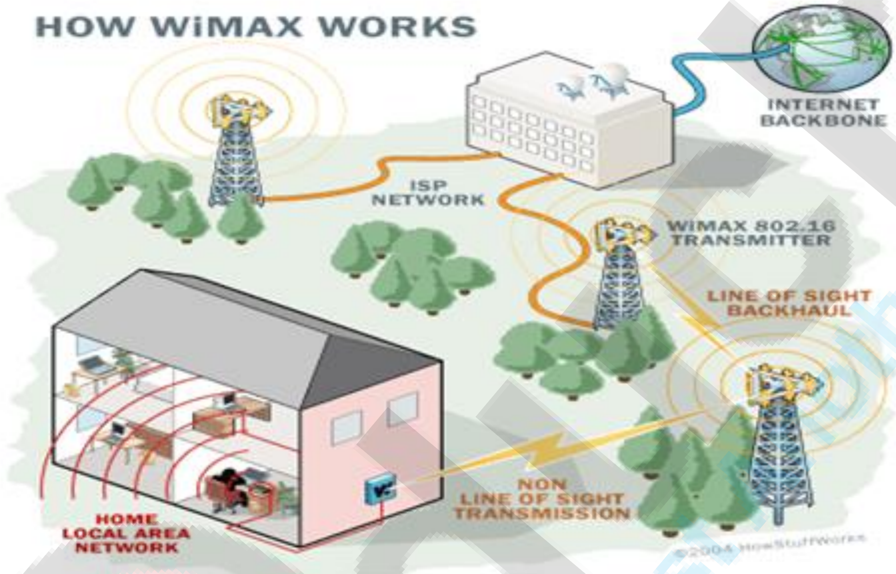
Q-4:-b->Discuss the architecture and services provided by IEEE 802.16??

Ans:-> WIMAX / IEEE 802.16:->

Wimax networks refer to broadband wireless networks that are based on the IEEE 802.16 standard, which ensures compatibility and interoperability between broadband wireless access equipment .

q The IEEE 802.16 standards define how wireless traffics move between subscriber equipment and core networks.

q WiMAX was designed for the transmission of multimedia services (voice, Internet, email, games and others) at high data rates.



802.16 Standards :->

	IEEE 802.16	IEEE 802.16a/802.16d	IEEE 802.16e
Completed	Dec 2001	Oct 2004	Dec 2005
Spectrum	10 - 66 GHz	2 – 11 GHz	2 - 6GHz
Application	Backhaul	Wireless DSL and Backhaul	Mobile Internet
Channel Conditions	Line of Sight Only	Non-Line of Sight	Non-Line of Sight
Bit Rate	32 – 134 Mbps	Up to 75 Mbps	Up to 15 Mbps
Modulation	QPSK,16QAM and 64QAM	OFDM ,QPSK,16QA M, 64QAM	OFDMA
Channel Bandwidths	20,25 and 28 MHz	1.5 and 20 MHZ	Same as 802.16d

The IEEE 802.16e-2005 standard provides the air interface for WiMAX but does not define the full end-to-end WiMAX network. The WiMAX Forum's Network Working Group (NWG) is responsible for developing the end-to-end network requirements, architecture, and protocols for WiMAX, using IEEE 802.16e-2005 as the air interface.

The WiMAX NWG has developed a network reference model to serve as an architecture framework for WiMAX deployments and to ensure interoperability among various WiMAX equipment and operators.

The network reference model envisions a unified network architecture for supporting fixed, nomadic, and mobile deployments and is based on an IP service model. Below is simplified illustration of an IP-based WiMAX network architecture.

The overall network may be logically divided into three parts:

Mobile Stations (MS) used by the end user to access the network.

The access service network (ASN), which comprises one or more base stations and one or more ASN gateways that form the radio access network at the edge.

Connectivity service network (CSN), which provides IP connectivity and all the IP core network functions.

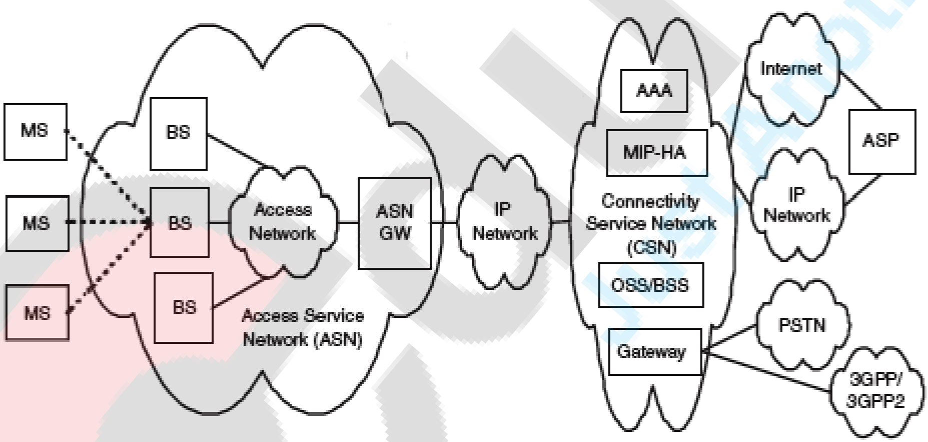
The network reference model developed by the WiMAX Forum NWG defines a number of functional entities and interfaces between those entities. Fig below shows some of the more important functional entities.

Base station (BS): The BS is responsible for providing the air interface to the MS. Additional functions that may be part of the BS are micromobility management functions, such as handoff triggering and tunnel establishment, radio resource management, QoS policy enforcement, traffic classification, DHCP (Dynamic Host Control Protocol) proxy, key management, session management, and multicast group management.

Access service network gateway (ASN-GW): The ASN gateway typically acts as a layer 2 traffic aggregation point within an ASN. Additional functions that may be part of the ASN gateway include intra-ASN location management and paging, radio resource management, and admission control, caching of subscriber profiles, and encryption keys, AAA client functionality, establishment, and management of mobility tunnel with base stations, QoS and policy enforcement, foreign agent functionality for mobile IP, and routing to the selected CSN.

Connectivity service network (CSN): The CSN provides connectivity to the Internet, ASP, other public networks, and corporate networks. The CSN is owned by the NSP and includes AAA servers that support authentication for the devices, users, and specific services. The CSN also provides per user policy management of QoS and security. The CSN is also responsible for IP address management, support for roaming between different NSPs, location management between ASNs, and mobility and roaming between ASNs.

IP-Based WiMAX Network Architecture



The WiMAX architecture framework allows for the flexible decomposition and/or combination of functional entities when building the physical entities. For example, the ASN may be decomposed into base station transceivers (BST), base station controllers (BSC), and an ASNGW analogous to the GSM model of BTS, BSC, and Serving GPRS Support Node (SGSN).

Q 5 A) Describe the WAP protocol Stack. What are the functions of different layers in this protocol stack.

WAP : WAP is the worldwide standard for providing Internet communications and advanced telephony services on digital mobile phones, pagers, personal digital assistants, and other wireless terminals - *WAP Forum.*
WAP stands for Wireless Application Protocol. Per the dictionary definition for each of these words we have:

- Wireless: Lacking or not requiring a wire or wires pertaining to radio transmission.
- Application: A computer program or piece of computer software that is designed to do a specific task.
- Protocol: A set of technical rules about how information should be transmitted and received using computers.

WAP is the set of rules governing the transmission and reception of data by computer applications on or via wireless devices like mobile phones. WAP allows wireless devices to view specifically designed pages from the Internet using only plain text and very simple black-and-white pictures.
WAP is a standardized technology for cross-platform, distributed computing very similar to the Internet's combination of Hypertext Markup Language (HTML) and Hypertext Transfer Protocol (HTTP), except that it is optimized for:
low-display capability
low-memory
low-bandwidth devices, such as personal digital assistants (PDAs), wireless phones, and pagers.
WAP is designed to scale across a broad range of wireless networks like GSM, IS-95, IS-136, and PDC.
WAP is designed in a layered fashion, so that it can be extensible, flexible, and scalable. As a result, the WAP protocol stack is divided into five layers:

Application Layer

Wireless Application Environment (WAE). This layer is of most interest to content developers because it contains among other things, device specifications, and the content development programming languages, WML, and WMLScript.

Session Layer

Wireless Session Protocol (WSP). Unlike HTTP, WSP has been designed by the WAP Forum to provide fast connection suspension and reconnection.

Transaction Layer

Wireless Transaction Protocol (WTP). The WTP runs on top of a datagram service, such as User Datagram Protocol (UDP) and is part of the standard suite of TCP/IP protocols used to provide a simplified protocol suitable for low bandwidth wireless stations.

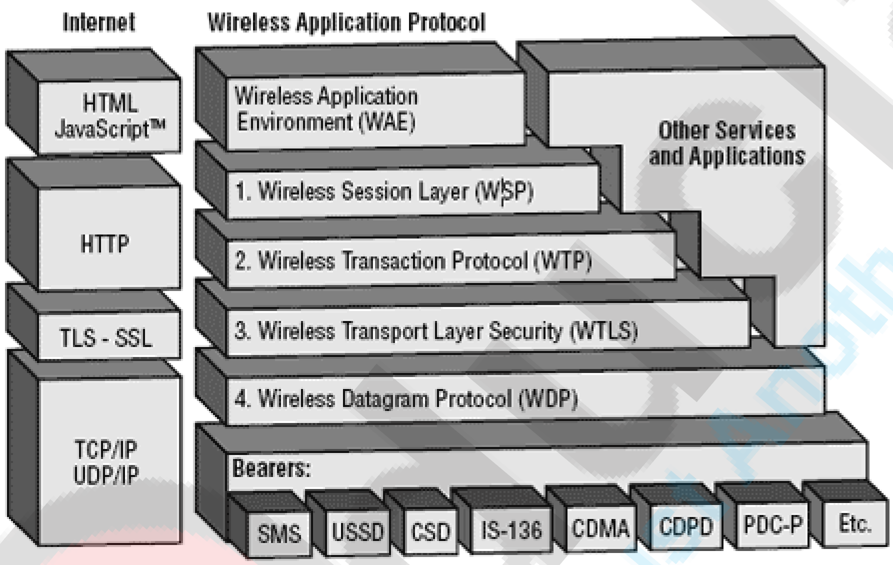
Security Layer

Wireless Transport Layer Security (WTLS). WTLS incorporates security features that are based upon the established Transport Layer Security (TLS) protocol standard. It includes data integrity checks, privacy, service denial, and authentication services.

Transport Layer

Wireless Datagram Protocol (WDP). The WDP allows WAP to be bearer-independent by adapting the transport layer of the underlying bearer. The WDP presents a consistent data format to the higher layers of the WAP protocol stack, thereby offering the advantage of bearer independence to application developers.

Each of these layers provides a well-defined interface to the layer above it. This means that the internal workings of any layer are transparent or invisible to the layers above it. The layered architecture allows other applications and services to utilise the features provided by the WAP-stack as well. This makes it possible to use the WAP-stack for services and applications that currently are not specified by WAP.



The WAP protocol architecture is shown below alongside a typical Internet Protocol stack.

Q 5 B) Why do you require spreading the spectrum? Explain the different methods of spreading the data and spectrum in a wireless environment.

Ans : As the name implies, spread spectrum techniques involve spreading the bandwidth needed to transmit data – which does not make sense at first sight. Spreading the bandwidth has several advantages. The main advantage is the resistance to narrowband interference. In following figure : Diagram

i) shows an idealized narrow band signal from a sender of user data (here power density dP/df versus frequency f).

The sender now spreads the signal in step ii), i.e., converts the narrowband signal into a broadband signal. The energy needed to transmit the signal (the area shown in the diagram) is the same, but it is now spread over a larger frequency range. The power level of the spread signal can be much lower than that of the original narrowband signal without losing data. Depending on the generation and reception of the spread signal, the power level of the user signal can even be as low as the background noise. This makes it difficult to distinguish the user signal from the background noise and thus hard to detect.

During transmission, narrowband and broadband interference add to the signal in step iii). The sum of interference and user signal is received. The receiver now knows how to despread the signal, converting the spread user signal into a narrowband signal again, while spreading the narrowband interference and leaving the broadband interference. In step v) the receiver applies a bandpass filter to cut off frequencies left and right of the narrowband signal. Finally, the receiver can reconstruct the original data because the power level of the user signal is high enough, i.e., the signal is much stronger than the remaining interference. The following sections show how spreading can be performed.

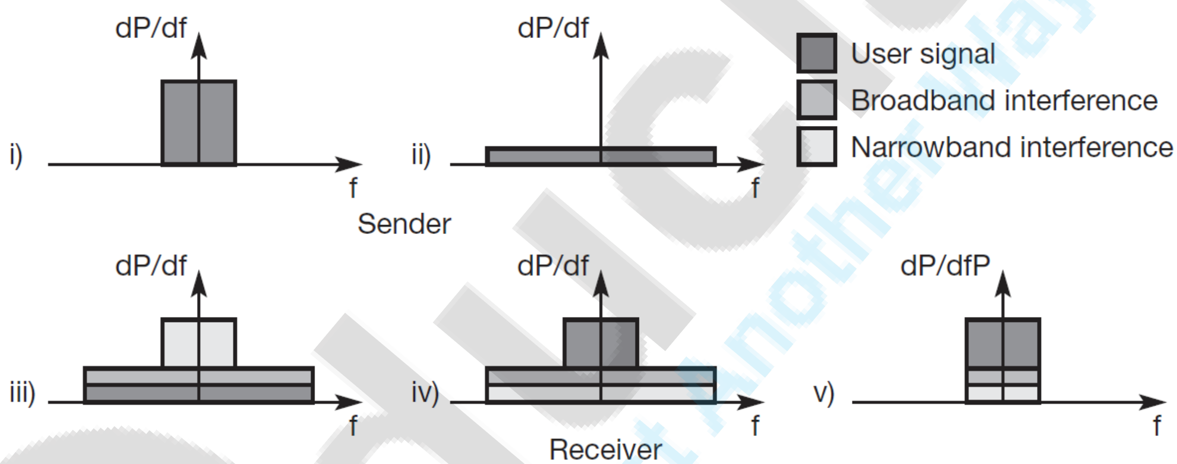


Fig. shows need of Spread Spectrums and its spreading and despreading

Just as spread spectrum helps to deal with narrowband interference for a single channel, it can be used for several channels.

Spreading the spectrum can be achieved in two different ways as shown in the following two sections.

Frequency Hopping Spread Spectrum (FHSS) has the frequency of the transmitted message periodically changed (or hopped). The transmitter hops frequencies according to a pre-set sequence (or hop sequence). The receiver either stays synchronized with the transmitter hopping, or is able to detect the frequency of each transmission.
FHSS can hop rapidly, several times per message, but generally it transmits a complete message (or data packet) and then hops. Each transmitter hops to a particular hop-sequence, which it

chooses automatically or is user-configured. Because the hop-sequences of different transmitters are different, the hopping of a "foreign" transmitter exhibits statistical randomness (though not truly random).

FHSS hopping sequences are pseudo-random, in that the probability of a foreign transmitter hopping to a particular channel appears to be random.
If more than one system hops onto the same channel, a "hop-clash" event, then those radio messages are corrupted. However when the transmitters hop again, the probability that both transmitters will hop to the same frequency a second time is very remote.

Direct Sequence Spread Spectrum (DSSS) differs from FHSS in that the transmitted data packet is "spread" across a wide-channel, effectively transmitting on multiple narrow channels simultaneously. When a data packet is transmitted, the data packet is modulated with a pseudorandom generated key, normally referred to as a "chipping-key", which spreads the transmission across the wide-band channel.
The receiver decodes and recombines the message using the same chipping key to return the data packet to its original state.
FHSS focuses the transmission power into one frequency channel at any one time. The first diagram shows a time-delayed spectrum-analysis of FHSS transmission – it shows three successive data packets transmitted on three channels – it does not indicate which of the three transmissions occurred first. The signal received is extremely large relative to the base background noise.
DSSS spreads the power of the transmitter across each channel. The result, as illustrated in the second diagram, is a wide span of low power transmissions. As a result of the low power transmissions, the distance capabilities as well as the penetrating power of the DSSS are greatly reduced when compared to FHSS, however the possible data rates for DSSS are much higher.

Q.6.A) What is the difference between GSM and GPRS? Explain the architecture of GPRS.

Ans: Difference Between GSM and GPRS

GSM	GPRS
1. GSM is Global System for Mobile Communications. 2. GSM is a wireless platform that uses radio frequencies. It has been designed for speech services and uses circuit switched transmission. 3. It is one of the leading digital cellular systems.	1. GPRS is General Packet Radio Service. 2. GPRS is a separate packet data network which provides a packet base platform both for the data transfer and signaling. 3. It is a standard for transferring data wirelessly.

4. Current GSM systems can transfer data up to 9.6kb/ps.	4. Current GPRS systems can transfer data up to 115 kb/ps.
5. GSM is considered as phone networks.	5. GPRS is a data service.
6. To access a GSM n/w , GSM capable phone is required. 7. GSM uses a combination of Frequency Division Multiple Access (FDMA) and Time Division Multiple Access(TDMA).	6. GPRS is a mobile data service available to users of GSM mobile phones. 7. GPRS is compatible with the standard TDMA scheme of GSM.
8. The GSM system uses LAPDm protocol in Data Link Layer.	8. GPRS uses LLC and RLC/MAC protocol in Data Link Layer.
9. GSM uses three protocols named Connection Management (CM), Mobility Management (MM) and Radio Resources (RR) at Network Layer.	9. GPRS uses the Subnetwork Dependent Convergence Protocol(SNDCP) at Network Layer.

<u>GPRS Architecture:</u>

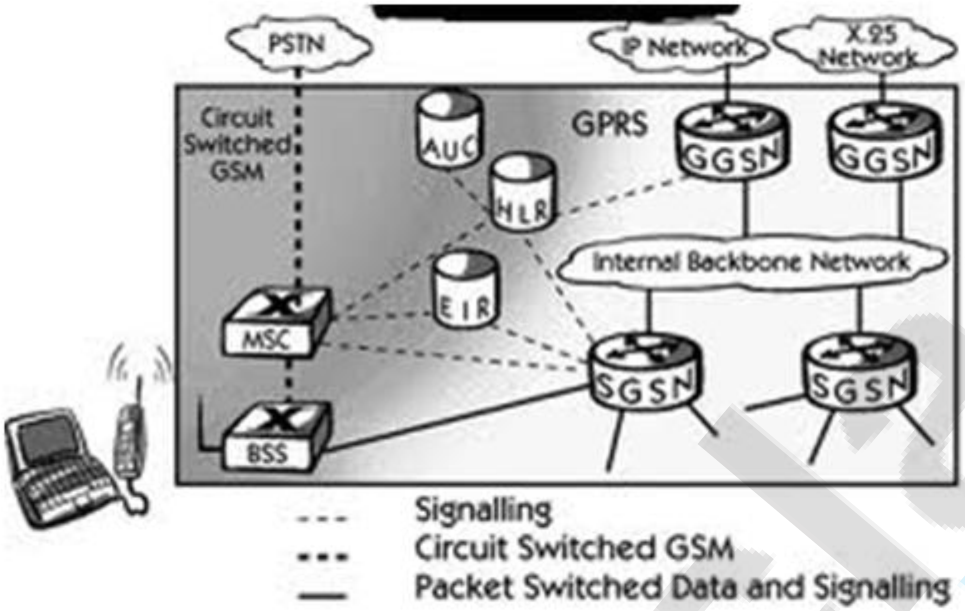
General packet Radio Service (GPRS) is a enhancement of GPS, which is packet oriented mobile data service on the 2G and 3G cellular communication system. It provide connection to the external packet data network through the GSM infrastructure with short access time to the network for independent short packets. It uses exactly uses the same physical radio channel as GSM and only new logical GPRS Radio Channel are defined. GPRS was originally standardized by European Telecommunications Standards Institute (ETSI) in response to the earlier CDPD & i-mode packet-switched cellular technologies. Here in this post, GPRS Architecture in Mobile Communication is explained in detail.

<u>GPRS Network Architecture:</u>

GPRS is usually attempts to reuse the existing GSM network elements as much as possible. There are new entities called GPRS that supports nodes (GSN) which are responsible for delivery and routing of data packets between mobile stations and external packets networks. There are two types of GSNs,

- Serving GPRS Support Node (SGNS)
- Gateway GPRS Support Node (GGNS)

These two modesare comparable to MD-IS in CPDP. There is also a new database called GPRS register which is located with HLR. It stores routing informations and maps the IMSI to a PDN address. Thus, GPRS Reference Architecture is shown as-



GPRS Network Architecture

Subsystems of GPRS Architecture

Mobile Station:

GPRS Services required New Mobile Station as the existing GSM phones are not capable of handling the enhanced air interface or the packet data. A wide variety of Mobile stations exist which includes a high-speed version of current phones to support high-speed data access like PC cards for laptop computers. These mobile stations are in backward compatibility mode in order to make voice calls which are used GSM.

Base Station Subsystem:

Each BSC requires the installation of Packet Control Units in addition to software upgrade. They provide physical and logical data interface to BSS to estimate packet data traffic. BTS too require a software upgrade but typically does not involve hardware enhancements.

When the traffic is originated at the subscriber mobile then it is transported over the air interface to BTS and then from BTS to BSC, the same way in standard GSM call. But at output of BSC the traffic is separated, the voice is sent to the mobile switching centre per standard GSM and the data is sent to the new device called the SGSN via the PCU.

GRPS Support Nodes:

- SSGN: The Serving GPRS Support Node is responsible for authentication of GPRS mobiles, registration of mobiles in the network, mobility management, and collecting information for charging for the use of the air interface.
- GGSN: The Gateway GPRS Support Node acts as an interface and a router to external networks. The GGSN contains routing information for GPRS mobiles, which is used to tunnel packets through the IP based internal backbone to the correct Serving GPRS Support Node.

Internal Back Network:

The internal backbone is an IP based network which is used to carry the new packets between different GSN. The process of Tunneling is used in-between SGSNs and GGSNs, this is done to safe exchange of domain informations outside the GPRS Network with out informing internal backbone.

Mobility Support:

In a manner similar to GSM and CDPD, there are mechanism in GPRS to support mobility.
There are two types of Mobility Support in GPRS Network-

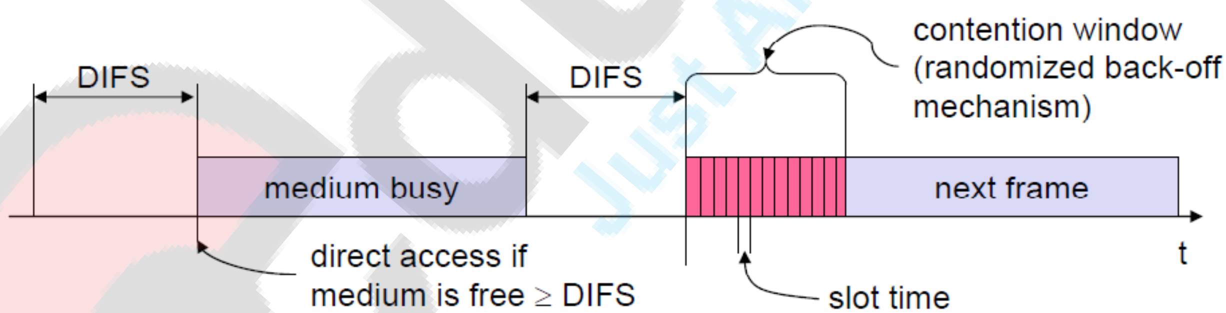
· Attachment Procedure
· Location and Handoff Management

Q.6

b) Discuss Mac layer in IEEE 802.11.

Avoid collisions: 2+ nodes transmitting at same time
 802.11: CSMA - sense before transmitting
don't collide with ongoing transmission by other node
 802.11: *no* collision detection!
difficult to receive (sense collisions) and transmitting at the same time because (TDD operation)
transmission and reception are at the same frequency
=> the station's receiver's will be overwhelming by it's own transmitting signals and thus can't hear the relatively "weak" signals sent by the others
 In general can't sense all collisions anyway, e.g. The Hidden terminal problem
=> Design Goal: *avoid collisions:* CSMA/C(ollision)A(voidance)

802.11 MAC CSMA/CA access method

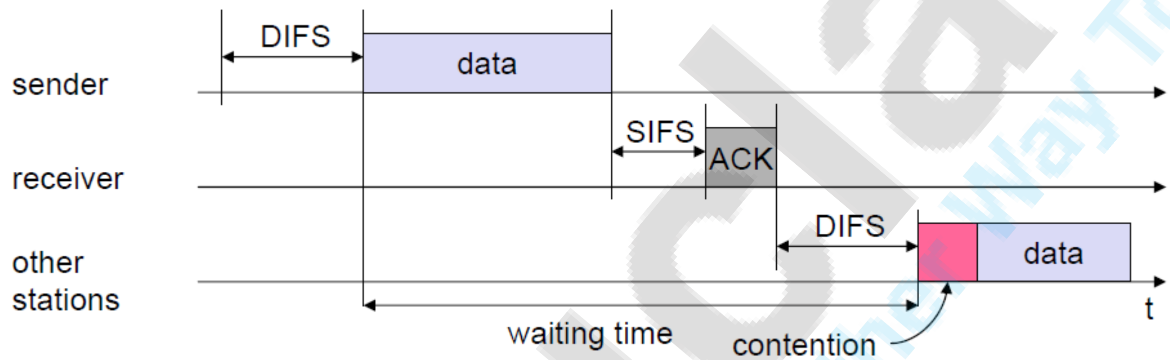


- station ready to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment).
- if the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending (IFS depends on service type).
- if the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time).

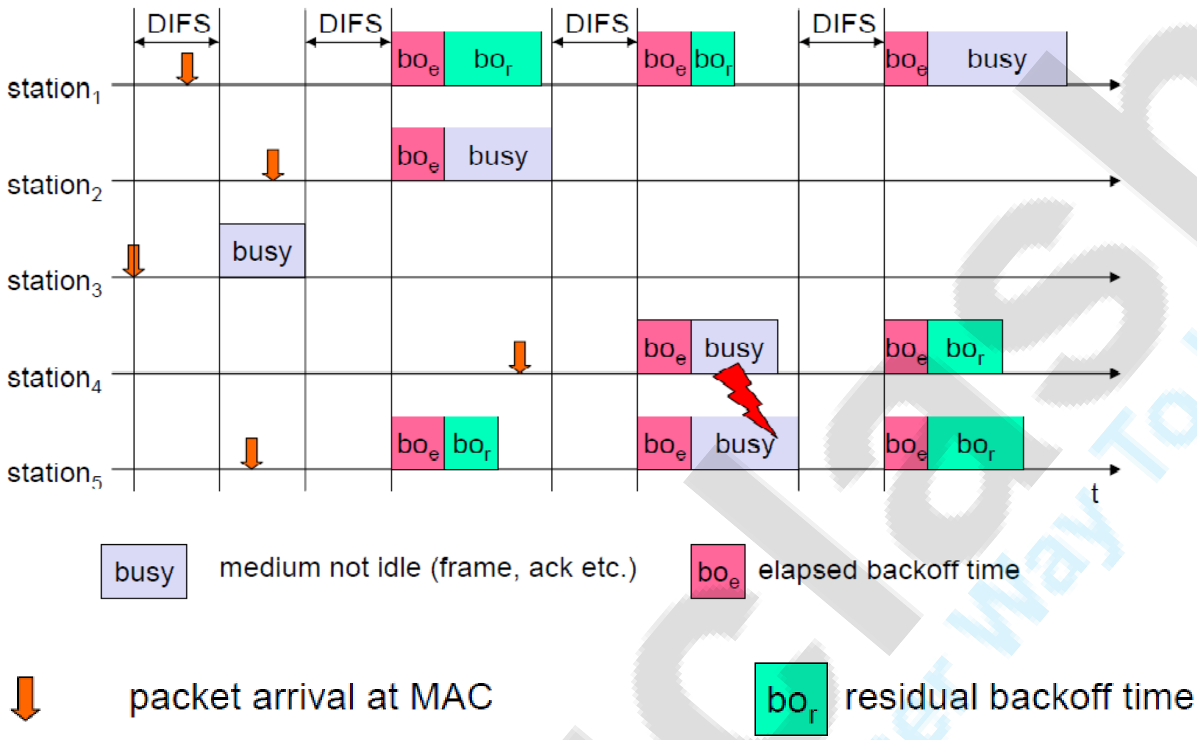
- if another station occupies the medium during the back-off time of the station, the back-off timer stops (fairness).

Sending unicast packets

- station has to wait for DIFS before sending data
- receivers acknowledge at once (after waiting for SIFS) if the packet was received correctly (CRC)
- automatic retransmission of data packets in case of transmission
- errors

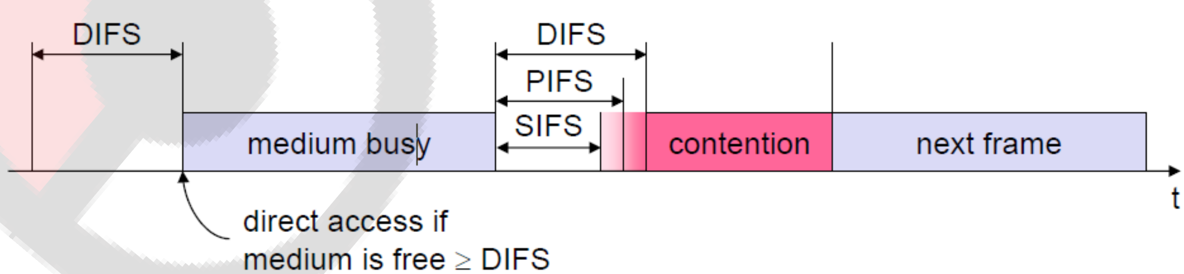


802.11 - competing stations - simple version



Priorities

- defined through different inter frame spaces (IFS)
- no guaranteed, hard priorities
- SIFS (Short Inter Frame Spacing)
  highest priority, for ACK, CTS, polling response
- PIFS (PCF IFS)
  medium priority, for time-bounded service using PCF
- DIFS (DCF, Distributed Coordination Function IFS)
  lowest priority, for asynchronous data service



MAC address format

scenario	to DS	from DS	address 1	address 2	address 3	address 4
ad-hoc network	0	0	DA	SA	BSSID	-
infrastructure network, from AP	0	1	DA	BSSID	SA	-
infrastructure network, to AP	1	0	BSSID	SA	DA	-
infrastructure network, within DS	1	1	RA	TA	DA	SA

DS: Distribution System
AP: Access Point
DA: Destination Address
SA: Source Address
BSSID: Basic Service Set Identifier (= MAC address of the AP)
RA: Receiver Address
TA: Transmitter Address

Q-7:->Write a short note on the following?
1). Antennas
ANS:-7-1:->Antennas
As the name wireless already indicates, this communication mode involves 'getting rid' of wires and transmitting signals through space without guidance.

· We do not need any 'medium' (such as an ether) for the transport of electromagnetic waves. Somehow, we have to couple the energy from the transmitter to the out-side world and, in reverse, from the outside world to the receiver.

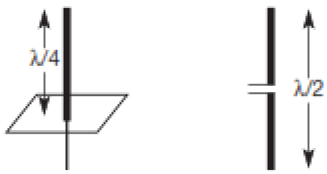
· This is exactly what antennas do. Antennas couple electromagnetic energy to and from space to and from a wire or coaxial cable (or any other appropriate conductor).

· Real antennas all exhibit directive effects, i.e., the intensity of radiation is not the same in all directions from the antenna.

The simplest real antenna is a thin, center-fed dipole, also called Hertzian dipole, as shown in Figure below. Thedipole consists of two collinear conductors of equal length, separated by a small feeding gap. The length of the dipoleis not arbitrary, but, for example,

· half the wavelength λ of the signal to transmit results in a very efficient radiation of the energy.

· If mounted on the roof of a car, the length of λ/4 is efficient. This is also known as Marconi antenna.



Types of Antennas

1) ½ Wave Dipole :
2) Directed Antenna :
3) Sectorized Antenna :

2). Symbian OS
Ans-7-ii):->symbian os:->

The Symbian OS is the operating system developed and sold by Symbian Ltd. The OS is used primarily by Nokia with its S60 user interface and by Sony Ericsson with its UIQ user interface, but the Symbian OS is also used by a number of Japanese mobile phone manufacturers for handsets sold inside of Japan. With Nokia's acquisition of Symbian, the Symbian OS is to be spun off into as an open source product offered by the newly formed Symbian Foundation.

basic principles.:->
-The integrity and security of user data
is paramount,
-user time must not be wasted,
-all resources are scarce.

Part of the Mobile Operating System :->
Written in C++.
Only runs on ARM processors

XHTML :
Extensible Hypertext Markup Language (XHTML) is a family of XML markup languages that mirror or extend versions of the widely used Hypertext Markup Language (HTML), the language in which Web pages are formulated.

While HTML, prior to HTML5, was defined as an application of Standard Generalized Markup Language (SGML), a flexible markup language framework, XHTML is an application of XML, a more restrictive subset of SGML. XHTML documents are well-formed and may therefore be parsed using standard XML parsers, unlike HTML, which requires a lenient HTML-specific parser.

There are various differences between XHTML and HTML. The Document Object Model (DOM) is a tree structure that represents the page internally in applications, and XHTML and HTML are two different ways of representing that in markup (serializations). Both are less expressive than the DOM (for example, "--" may be placed in comments in the DOM, but cannot be represented in a comment in either XHTML or HTML), and generally XHTML's XML syntax is a little more expressive than HTML (for example, arbitrary namespaces are not allowed in HTML). First off, one source of differences is immediate: XHTML uses an XML syntax, while HTML uses a pseudo-SGML syntax (officially SGML for HTML 4 and under, but never in practice, and standardised away from SGML in HTML5). Secondly however, because the expressible contents of the DOM in syntax are slightly different, there are some changes in actual behavior between the two models.

Impairments in Wireless Transmission :

Wireless impairments generally fall in to one of two categories. Intervening materials between the transmitter and receiver that block the signal and actual interference of the signal. Usually the intervening materials problem can be overcome by repositioning the antennas or boosting the signal. Interference can come in many forms, other wireless signals on the same or nearby channels is very common, wireless cameras and phones are examples.

Spurious radiation within the bandwidth from microwave ovens and the like can also be a big problem. These issues can be harder to deal with especially when the problem comes and goes. Changing channels will often deal with the issue, other times you need to elimenate the source of the interference.

Performance Criterion How a “good” communication system can be differentiated from a “sloppy” one?For analog communications ˆ – How close is m(t) to m(t) Fidelity! – SNR is typically used as a performance metric For digital communications – Data rate and probability of error – No channel impairments, no error – With noise, error probability depends upon data rate, signal and noise powers, modulation scheme