WIRELESS TECHNOLOGY & MOBILE COMPUTING

As per syllabus of

MCA SEMESTER 5

(Mumbai University)

Compiled by

MissionMca.com

(For private circulation only)

Q 2) 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.

Amplitude shift keying:

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 infra red transmission, using a directed beam or diffuse light.

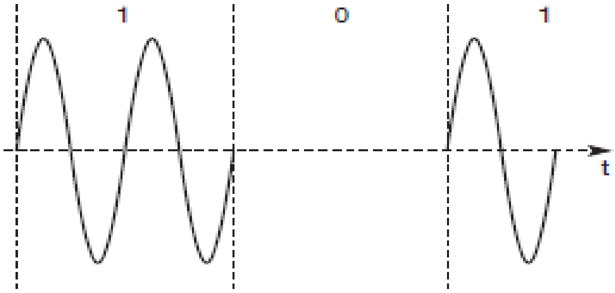


Figure 1. Amplitude shift keying (ASK)

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 an undesired side-effect.

A simple way to implement demodulation is by using two band pass filters, one for f1 the other for 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.

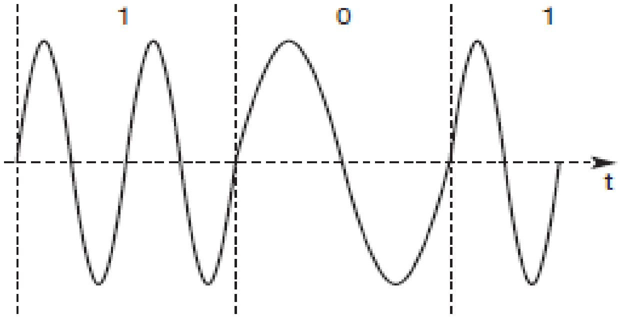


Figure 2. Frequency shift keying (FSK)

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.

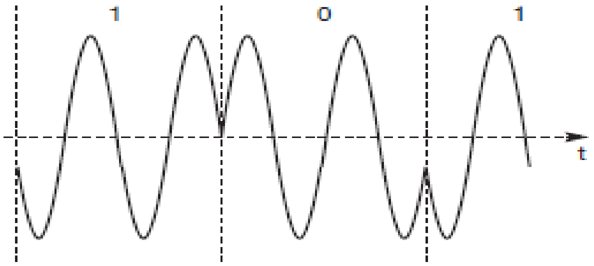


Figure 3. Phase shift keying (PSK)

Q 3) Explain the various configurations and the profiles supported in J2ME.

Ans: Traditional computing devices use fairly standard hardware configurations such as a display, keyboard, mouse, and large amounts of memory and permanent storage. However, the new breed of computing devices lacks hardware configuration continuity among devices. Some devices don't have a display, permanent storage, keyboard, or mouse. And memory availability is inconsistent among small computing devices.

The lack of uniform hardware configuration among the small computing devices poses a formidable challenge for the Java Community Process Program, which is charged with developing standards for the JVM and the J2ME for small computing devices.

J2ME must service many different kinds of small computing devices, including screen phones, digital set-top boxes used for cable television, cell phones, and personal digital assistants. The challenge for the Java Community Process Program is to develop a Java standard that can be implemented on small computing devices that have nonstandard hardware configurations.

The Java Community Process Program has used a twofold approach to addressing the needs of small computing devices. First, they defined the Java run-time environment and core classes that operate on each device. This is referred to as the *configuration*. A configuration defines the Java Virtual Machine for a particular small computing device. There are two configurations, one for handheld devices and the other for plug-in devices. Next, the Java Community Process Program defined a profile for categories of small computing devices.

A *profile* consists of classes that enable developers to implement features found on a related group of small computing devices.

J2ME Configurations:

There are two configurations for J2ME.

Connected Limited Device Configuration (CLDC)

The CLDC is designed for 16-bit or 32-bit small computing devices with limited amounts of memory. CLDC devices usually have between 160KB and 512KB of available memory and are battery powered. They also use an inconsistent, small-bandwidth network wireless connection and may not have a user interface. CLDC devices use the KJava Virtual Machine (KVM) implementation, which is a stripped-down version of the JVM. CLDC devices include pagers, personal digital assistants, cell phones, dedicated terminals, and handheld consumer devices with between 128KB and 512KB of memory.

Connected Device Configuration (CDC)

CDC devices use a 32-bit architecture, have at least two megabytes of memory available, and implement a complete functional JVM. CDC devices include digital set-top boxes, home appliances, navigation systems, point-of-sale terminals, and smart phones.

J2ME Profiles:

A profile consists of Java classes that enable implementation of features for either a particular small computing device or for a class of small computing devices.

■Foundation Profile :

The Foundation Profile is used with the CDC configuration and is the core for nearly all other profiles used with the CDC configuration because the Foundation Profile contains core Java classes.

■Game Profile :

The Game Profile is also used with the CDC configuration and contains the necessary classes for developing game applications for any small computing device that uses the CDC configuration.

■Mobile Information Device Profile :

The Mobile Information Device Profile (MIDP) is used with the CLDC configuration and contains classes that provide local storage, a user interface, and networking capabilities to an application that runs on a mobile computing device such as Palm OS devices. MIDP is used with wireless Java applications.

■PDA Profile :

The PDA Profile (PDAP) is used with the CLDC configuration and contains classes that utilize sophisticated resources found on personal digital assistants. These features include better displays and larger memory than similar resources found on MIDP mobile devices.

■Personal Profile :

The Personal Profile is used with the CDC configuration and the Foundation Profile and contains classes to implement a complex user interface. The Foundation Profile provides core classes, and the Personal Profiles provide classes to implement a sophisticated user interface, which is a user interface that is capable of displaying multiple windows at a time.

■Personal Basis Profile:

The Personal Basis Profile is similar to the Personal Profile in that it is used with the CDC configuration and the Foundation Profile. However, the Personal Basis Profile provides classes to implement a simple user interface, which is a user interface that is capable of displaying one window at a time.

■RMI Profile:

The RMI Profile is used with the CDC configuration and the Foundation Profile to provide Remote Method Invocation classes to the core classes contained in the Foundation Profile.

There will likely be many profiles as the proliferation of small computing devices continues. Industry groups within the Java Community Process Program (java.sun.com/about java/community process) define profiles. Each group establishes the standard profile used by small computing devices manufactured by that industry.

A CDC profile is defined by expanding upon core Java classes found in the Foundation Profile with classes specifically targeted to a class of small computing device. These device-specific classes are contained in a new profile that enables developers to create industrial-strength applications for those devices. However, if the Foundation Profile is specific to CDC, not all profiles are expanded upon the core classes found in the Foundation Profile.

Applications can access a small computing device's software and hardware features only if the necessary classes to do so are contained in the JVM and in the profile used by the developer.

Q4). Explain CDMA with suitable example. How is W-CDMA different from CDMA?

Ans:

CDMA (Code Division Multiple Access):

Codes with certain characteristics can be applied to the transmission to enable the use of Code Division Multiplexing (CDM).CDMA systems use exactly these codes to separate different users in code space and to enable access to a shared medium without interference. CDMA refers to the any of several protocols used in Second Generation (2G) and Third Generation (3G) wireless communication. CDMA is a form of multiplexing, allowing numerous signals to use 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. In CDMA all terminals can be active at the same place at the same moment, and they are uninterrupted.

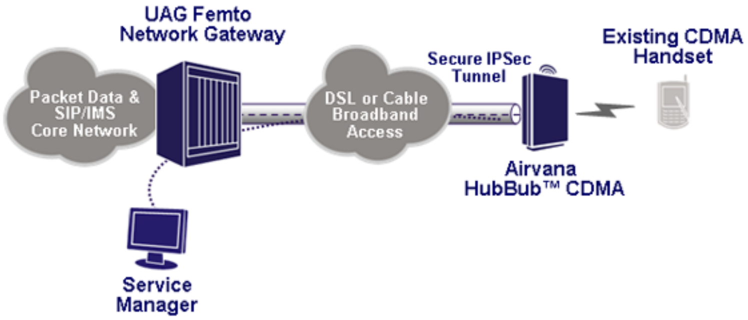


Fig: CDMA

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 patterned, so it can be intercepted only by a receiver whose frequency response is programmed with the same code. The CDMA channel is nominally 1.23 MHz wide. CDMA networks use a scheme called soft hand-off, which minimizes signal breakup as a handset passes from one cell to another. The combination of digital and spread spectrum modes support several times as many signals per unit bandwidth as analog modes. CDMA is compatible with other cellular technologies which allows for nationwide Roaming. The original CDMA standard, also known as CDMA One and still common in cellular telephones, offers a transmission speed of only up to 14.4Kbps in its single channel form and up to 115Kbps in an eight channel form. CDMA2000 and Wideband CDMA (W-CDMA) deliver data many times faster.

Following example explain basic function of CDMA before it is applied to signals:

1. Two senders, A and B, want to send data. CDMA assigns the following unique and orthogonal key sequences: key A_k =010011 for sender A, key B_k =110101 for sender B. sender A wants to send the bit A_d =1, sender B sends B_d =0. Let us assume that we code binary 0 as -1, a binary 1 as +1, and then apply the standard addition and multiplication rules.
2. Both senders spread their signal using their key as chipping sequence. Sender A sends the signal $A_s = A_d * A_k = +1*(-1,+1,-1,-1, +1,+1) = (-1,+1,-1,-1,+1,+1)$. Sender B does the same with its data to spread the signal with the code:
   $B_s = B_d* B_k= -1*(+1,+1,-1,+1,-1,+1) = (-1,-1,+1,-1,+1,-1)$.
3. Both signals are then transmitted at the same time using the same frequency, so, the signals superimpose in space. Assume that the signals have the same strength at the receiver, the following signal C is received at a receiver: $C = A_s + B_s = (-2, 0, 0,-2, +2, 0)$.
4. The receiver now wants to receive data from sender A and, therefore, tunes in to the code of A, i.e., applies A's code for dispreading $C*A_k =(-2, 0, 0, -2, +2, 0)*(-1,+1,-1,-1,+1,+1) = 2+0+0+2+2+0 = 6$. Result is much larger than 0, the receiver detects binary 1.Tuing in the sender B, i.e., applying B's code gives $C*B_k = (-2, 0, 0, -2, +2, 0)*(+1, +1, -1, +1, -1, +1) = -2+0+0-2-2+0 = -6$. The result is negative i.e. less than 0, the receiver detects binary 0.

The Advantage of CDMA is-

Flexible, less planning needed, soft handover.

The Disadvantage of CDMA is-

Complex Receivers, needs more complicated power control for senders.

WCDMA (Wideband CDMA):

WCDMA is the radio access scheme used for Third Generation cellular systems that are being rolled out in various parts of the globe. The 3G systems to support wideband services like high-speed Internet Access, video and high quality image transmission with the same quality as the fixed networks. In WCDMA systems the CDMA air interface is combined with GSM based networks. The WCDMA standard was evolved through the Third Generation Partnership Project (3GPP) which aims to ensure interoperability between different 3G networks.

In WCDMA, there are two different modes of operation possible:

1. TDD: In this duplex method, uplink and downlink transmission are carried over the same frequency band by using synchronized time intervals. Thus time slots in a physical channel are divided into transmission and reception part.
2. FDD: The uplink and downlink transmission employ two separated frequency bands for this duplex method. A pair of frequency bands with specified separation is assigned for connection.

WCDMA is different from CDMA in following ways

	WCDMA	**CDMA**
Bandwidth	5 MHz	1.25MHz
Chip rate	3.84 Mcps	1.2288 Mcps
Speed	Faster than CDMA	Slower than WCDMA
Technology	3G	2G
Base station synchronization	Not needed	Yes, via GPS
Cell search	3-step approach via primary, secondary search code and CPICH	Sync through time-shifted short code correlation
User separation	CDM / TDM (shared channel)	1xRTT: CDM 1xEV-DO: TDM (scheduler)
2G interoperability	GSM-UMTS handover (Multi-mode terminals)	1xRTT backward compatible (1xEV-DO not)

Q 5) Explain the various states that a Bluetooth enabled device can move into

Ans:

Active Mode:

In this mode, the Bluetooth module participates actively on the transmission channel. The master regularly sends a packet to the slaves (polling) to enable the slaves to be able to send a packet to the master and re-synchronise themselves. In this type of mode, the consumption of a Bluetooth module (in transmission) is around 40mA to 50mA (depending on the transmission output).

Sniff Mode: This is a low consumption mode. A Bluetooth module in the Sniff mode stays synchronised in the piconet. It listens to the piconet at regular intervals (Tsniff) for a short instant. This enables it to re-synchronise itself with the piconet and to be able to make use of this Sniff window to send or receive data. The consumption is as low as the Tsniff is large (compared to the Sniff window). If Tsniff is in the region of a second and the duration of Sniff (Twin) is in the region of several ms, the consumption will be about 1 to 5% of the maximum transmission consumption. (average consumption of 1mA to 5mA approximately). The Baracoda reader generally maintains the connection between 2 consecutive scans. However, for reasons of consumption, the scanner puts itself into the Sniffmode; Tsniff is regularly re-negotiated between the scanner and the terminal in such a way that the Tsniff increases as the time without a scan passes. The advantage of a large Tsniff is the low consumption and the inconvenience is the delay in sending the bar code.

The algorithm developed by Baracoda allows the definition of the best Tsniff, a compromise between low consumption and short delay. This compromise adapts itself to the user (scan statistic). The advantage in maintaining the connection is to avoid a Paging / Create Connection phase which is responsible for high energy consumption.

Hold Mode:

The module remains synchronized. This is lower consumption mode than the Sniff mode. Only the counter on the Bluetooth chip in hold mode is active. At the end of the Hold period, the Bluetooth module returns to the active mode.

Park Mode:

A Bluetooth module in this mode is no longer an active member of the piconet. However, it remains synchronized with the master and can listen to a broadcast channel (Beacon Channel).

Q 6) Why is FEC necessary in wireless data communication? What are block codes and convolution codes? Explain the (n, k, K) convolution code, what do n k and K represent? Draw an encoder with values (2, 1, 3).

Ans: In telecommunication, information theory, and coding theory, **forward error correction FEC)** or channel coding is a technique used for controlling errors in data transmission over unreliable or noisy communication channels. The central idea is the sender encodes their message in a redundant way by using an error-correcting code (ECC). The American mathematician Richard Hamming pioneered this field in the 1940s and invented the first error-correcting code in 1950: the Hamming (7,4) code.

The term *forward* refers to procedures whereby a receiver, using only information contained in the incoming digital transmission, corrects bit errors in the data. This is in contrast to backward error correction, in which the receiver merely detects the presence of errors and then sends a request back to the transmitter to retransmit the data in error. Backward error correction is not practical in many wireless applications. For example, in satellite communications, the amount of delay involved makes retransmission undesirable. In Mobile communications, the error rates are often so high that there is a high probability that the retransmitted block of bits will also contain errors. In these applications, forward error correction is required

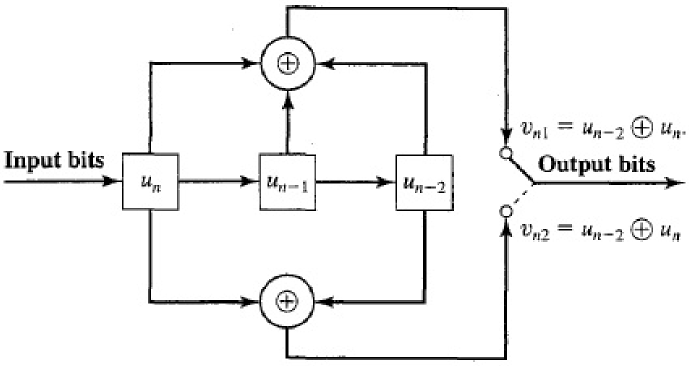
Convolution Codes:

Block codes are one of the two widely used categories of error correcting codes for wireless transmission; the other is convolutional codes. An *(n, k)* block code process data in blocks of *k* bits at a time, producing a block of *n* bits *(n > k)* as output for every block of *k* bits as input. If data are transmitted and received in a more or less continuous stream, a block code, particularly one with a large value of *n,* may not be as convenient as a code that generates redundant bits continuously so that error checking and correcting are carried out continuously. This is the function of convolution codes.

A convolutional code is defined by three parameters: *n, k,* and *K.* An *(n, k, K)* code processes input data *k* bits at a time and produces an output of *n* bits for each incoming *k* bits. So far this is the same as the block code. In the case of a convolutional code, nand *k* are generally quite small numbers. The difference is that convolutional codes have memory, which is characterized by the *constraint factor K.* In essence, the current *n-bit* output of an *(n, k, K)* code depends not only on the value of the current block of *k* input bits but also on the previous *K* - 1 blocks of *k* input bits. Hence, the current output of *n* bits is a function of the last *K* X *k* input bits. Convolutional codes are best understood by looking at a specific example For an *(n, k, K)* code, the shift register contains the most recent *K* X *k* input bits; the register is initialized to all zeros.6 The encoder produces *n* output bits, after which the oldest *k* bits from the register are discarded and *k* new bits are shifted in. Thus, although the output of *n* bits depends on *K* X *k* input bits, the rate of encoding is *n* output bits per *k* input bits. As in a block code, the code rate is therefore *kin.* The most commonly used binary encoders have *k* = 1 and hence a shift register length of *K.* Our example is of a (2, 1,3) code (Figure 8.9a).

In this example, the encoder converts an input bit *Un* into two output bits *Vnl* and *Vn2,*using the three most recent bits. The first output bit produced is from the upper logic circuit *(Vnl = Un* E9 *Un-l* E9 *Un -2),* and the second output bit from the lower logic circuit *(Vn2 = Un*

E9 *Un -2).* For any given input of *k* bits, there are *2k(K-l)* different functions that map the *k* input bits into *n* output bits. Which function is used depends on the history of the last *(K* - 1) input blocks of *k* bits each. We can therefore represent a convolutional code using a finite-state machine. The machine has *2k(K-l)* states, and the transition from one state to another is determined by the most recent *k* bits of inputs and produces *n* output bits. The initial state of the machine corresponds to the all-zeros state. For our example (Figure 8.9b) there are 4 states, one for each possible pair of values for the last two bits. The next input bit causes a transition and produces an output of two bits. For example, if the last two bits were 10 *(Un-l* = 1, *Un -2* = 0) and the next bit is 1 *(Un* = 1), then the current state is state b (10) and the next state is
d (11).
The output is *Vnl* = *Un -2* EB *Un-l* EB *Un* = 0 EB 1 EB 1 = 0 *Vn2* = 0 EB 1 = 1



<u>Block codes</u>:

In coding theory, block codes are one of the two common types of channel codes (the other one being convolutional codes), which enable reliable transmission of digital data over unreliable communication channels subject to channel noise.

A block code transforms a message m consisting of a sequence of information symbols over an alphabet Σ into a fixed-length sequence c of n encoding symbols, called a code word. In a linear block code, each input message has a fixed length of $k < n$ input symbols. The redundancy added to a message by transforming it into a larger code word enables a receiver to detect and correct errors in a transmitted code word, and – using a suitable decoding algorithm – to recover the original message. The redundancy is described in terms of its information rate, or more simply – for a linear block code – in terms of its code rate, *k*/*n*.

The error correction performance of a block code is described by the minimum Hamming distance *d* between each pair of code words, and is called the *distance* of the code.

The encoder for a block code divides the information sequence into *message blocks*, each message block contains k information symbols over an alphabet set Σ, i.e. a message could be represented as a k-tuple $m = (m_1, m_2, \ldots, m_k) \in \Sigma^k$. The total number of possible different message is therefore | Σ | k. The encoder transforms message m independently onto an n-tuple codeword $c = (c_1, c_2, \ldots, c_n) \in \Sigma^n$. The code of block length n over Σ is a subset of Σn : the total number of possible different codewords is the same as the total number of messages | Σ | k and k is called dimension. Rate of the block code is defined as $R = \frac{k}{n}$.

The Hamming weight wt(c) of a codeword $c$is defined as the number of non-zero positions in c. The Hamming distance Δ(c1,c2) between two codewords c1 and c2 is defined as the number of different positions between the codewords. The (minimum) distance d of a block code $C \subseteq \Sigma^n$is defined as the minimum distance between any two different codewords: $d = \min_{c_1 \neq c_2 \in C} \Delta(c_1, c_2)$. The notation (n,k,d)Σ is used to represent a block code of dimension k, block length n over alphabet set Σ, with distance d. In particular, if alphabet set Σ has size q, the block code is denoted as (n,k,d)q.

Q 7) What is fading? Explain the types of fading. How does fading effect the wireless transmission?

Ans: The term *fading* refers to the time variation of received signal power caused by changes in the transmission medium or path(s).
In a fixed environment, fading is affected by changes in atmospheric conditions, such as rainfall. But in a mobile environment, where one of the two antennas is moving relative to the other, the relative location of various obstacles changes over time, creating complex transmission effects. 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. Fading effects in a mobile environment can be classified as either fast or slow.

The terms slow and fast fading refer to the rate at which the magnitude and phase change imposed by the channel on the signal changes. The coherence time is a measure of the minimum time required for the magnitude change of the channel to become uncorrelated from its previous value. Alternatively, it may be defined as the maximum time for which the magnitude change of channel is correlated to its previous value.

Slow fading arises when the coherence time of the channel is large relative to the delay constraint of the channel. In this regime, the amplitude and phase change imposed by the channel can be considered roughly constant over the period of use. Slow fading can be caused by events such as shadowing, where a large obstruction such as a hill or large building obscures the main signal path between the transmitter and the receiver. The amplitude change caused by shadowing is often modeled using a log-normal distribution with a standard deviation according to the log-distance path loss model.

Fast fading occurs when the coherence time of the channel is small relative to the delay constraint of the channel. In this regime, the amplitude and phase change imposed by the channel varies considerably over the period of use.

In a fast-fading channel, the transmitter may take advantage of the variations in the channel conditions using time diversity to help increase robustness of the communication to a temporary deep fade. Although a deep fade may temporarily erase some of the information transmitted, use of an error-correcting code coupled with successfully transmitted bits during other time instances (interleaving) can allow for the erased bits to be recovered.

In a slow-fading channel, it is not possible to use time diversity because the transmitter sees only a single realization of the channel within its delay constraint. A deep fade therefore lasts the entire duration of transmission and cannot be mitigated using coding.

Fading can cause poor performance in a communication system because it can result in a loss of signal power without reducing the power of the noise. This signal loss can be over some or all of the signal bandwidth. Fading can also be a problem as it changes over time: communication systems are often designed to adapt to such impairments, but the fading can change faster than the adaptations can be made. In such cases, the probability of experiencing a fade (and associated bit errors as the signal-to-noise ratio drops) on the channel becomes the limiting factor in the link's performance.

The effects of fading can be combated by using diversity to transmit the signal over multiple channels that experience independent fading and coherently combining them at the receiver. The probability of experiencing a fade in this composite channel is then proportional to the probability that all the component channels simultaneously experience a fade, a much more unlikely event.

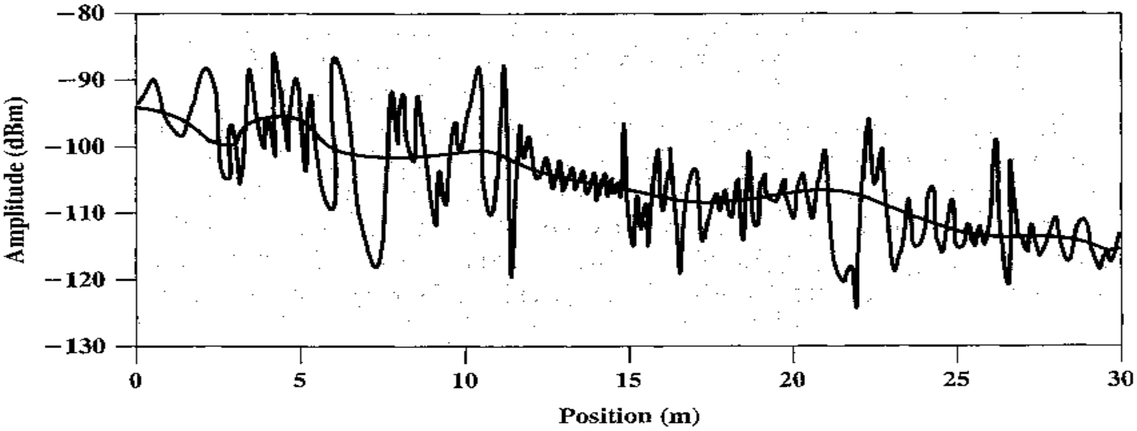


Figure 5.13 Typical Slow and Fast Fading in an Urban Mobile Environment

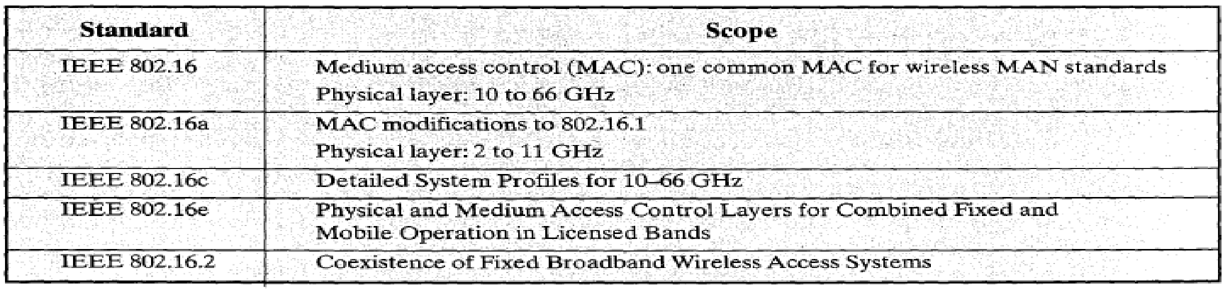
Q 8) Discuss the architecture and the services provided by the IEEE 802.16 protocol for wireless broadband in detail.

Ans:

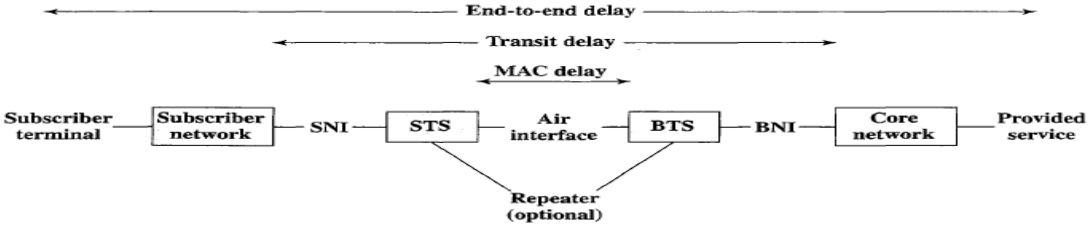
System Reference Architecture:

The 802.16 standards are designed with respect to the abstract system reference model shown in Figure 11.13. An 802.16 wireless. service provides a communications path between a subscriber site, which may be either a single subscriber device or a network on the subscriber's premises (e.g., a LAN, PBX, IP-based network) and a core network (the network to which 802.16 is providing access).

IEEE 802.16 Standards



Standard	Scope
IEEE 802.16	Medium access control (MAC): one common MAC for wireless MAN standards Physical layer: 10 to 66 GHz
IEEE 802.16a	MAC modifications to 802.16.1 Physical layer: 2 to 11 GHz
IEEE 802.16c	Detailed System Profiles for 10–66 GHz
IEEE 802.16e	Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands
IEEE 802.16.2	Coexistence of Fixed Broadband Wireless Access Systems



SNI: STS network interface
STS: Subscriber transceiver station
BTS: Base transceiver station
BNI: BTS network interface

IEEE 802.16 System Reference Points

Examples of a core network are the public telephone network and the Internet. Three interfaces are defined in this model. IEEE 802.16 standards are concerned with the air interface between the subscriber's transceiver station and the base transceiver station. The standards specify all the details of that interface. The system reference model also shows interfaces between the transceiver stations and the networks behind them (SNI and BNI). The reason for showing these interfaces in the system reference model is that the subscriber and core network technologies (such as voice, ATM, etc.) have an impact on the technologies used in the air interface and the services provided by the transceiver stations over the air interface.

Protocol Architecture:

Protocols defined specifically for wireless transmission address issues relating to the transmission of blocks of data over the network. In OSI terms, higher-layer protocols (layer 3 or

4 and above; see Figure 4.3) are independent of network architecture and are applicable to a variety of networks and communications interfaces. Thus, a discussion of 802.16 protocols is concerned with lowest two layers of the OSI model.

Figure below relates the four protocol layers defined in the 802.16 protocol architecture to the OSI model. Working from the bottom up, the lowest two layers of the 802.16 protocol model correspond to the physical layer of the OSI model and include such functions as

- Encoding/decoding of signals
- Preamble generation/removal (for synchronization)
- Bit transmission/reception

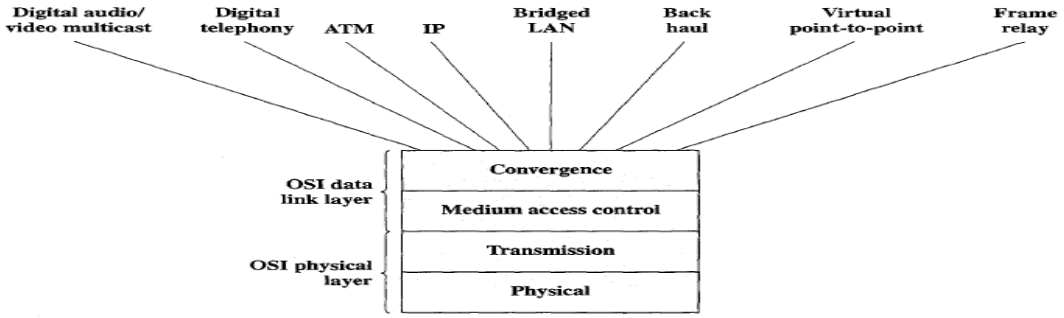


Figure IEEE 802.16 Protocol Architecture

In general, the 802.16 physical layer is concerned with these medium-dependent issues, and the transmission layer is concerned with the bulleted items listed previously. Above the physical and transmission layers are the functions associated with providing service to subscribers. These include :

- On transmission, assemble data into a frame with address and error detection fields.
- On reception, disassemble frame, and perform address recognition and error detection.
- Govern access to the wireless transmission medium.

These functions are grouped into a medium access control (MAC) layer. The protocol at this layer, between the base station and the subscriber station, is responsible for sharing access to the radio channel. Specifically, the MAC protocol defines how and when a base station or subscriber station may initiate transmission on the channel. Because some of the layers above the MAC layer, such as ATM, require specified service levels (QoS), the MAC protocol must be able to allocate radio channel capacity so as to satisfy service demands.

Above the MAC layer is a convergence layer that provides functions specific to the service being provided. A convergence layer protocol may do the following:

- Encapsulate PDU (protocol data unit) framing of upper layers into the native 802.16 MACIPHY frames.
- Map an upper layer's addresses into 802.16 addresses.
- Translate upper layer QoS parameters into native 802.16 MAC format.
- Adapt the time dependencies of the upper layer traffic into the equivalent MAC service.

Services:

Requirements for the IEEE 802.16 standards are defined in terms of bearer services that the 802.16 systems must support. A bearer service refers to the type of traffic generated by a subscriber network or core network in Figure 11.13. For example, an 802.16 interface must be able to support the data rate and QoS required by an ATM network or an IP-based network, or support the data rate and delay requirements of voice or video transmissions.

IEEE 802.16 is designed to support the following bearer services:

- Digital audio/video multicast: Transports one-way digital audio/video streams to subscribers. The principal example of this service is a broadcast radio and video similar to digital broadcast cable TV and digital satellite TV
- Digital telephony: Supports multiplexed digital telephony streams. This service is a classic WLL service that provides a replacement for wired access to the public telephone network.
- ATM: Provides a communications link that supports the transfer of ATM cells as part of an overall ATM network. The 802.16 link must support the various QoS services defined for ATM.
- Internet protocol: Supports the transfer of IP datagrams. The 802.16 link must provide efficient timely service. In addition, a variety of QoS services are now defined for IP-based networks, and 802.16 should support these.
- Bridged LAN: Similar to the IP-based support. A bridge LAN service enables transfer of data between two LANs with switching at the MAC layer.
- Back-haul: For cellular or digital wireless telephone networks. An 802.16 system may be a convenient means to provide wireless trunks for wireless telephony base stations.
- Frame relay: Similar to ATM. Frame relay uses variable-length frames in contrast to the fixed-length cells of ATM.

Bearer services are grouped in three broad categories:

- Circuit based: These services provide a circuit-switching capability, in which connections are set up to subscribers across a core network.
- Variable packet: IP and frame relay are examples of services that make use of variable-length PDUs. Another example is MPEG video, which is a video compression scheme in which successive blocks of digital video information may be of varying sizes.
- Fixed-length cell/packet: This service is for ATM.

Figure (IEEE 802.16 System Reference Points) shows three categories of delay defined in the 802.16 standards:

- Medium access delay: Once a transceiver station is ready to transmit, the medium access delay measures the amount of time that the station must wait before it can transmit.
- Transit delay: This is the delay from SNI to BNI or BNI to SNI. It includes the medium access delay plus the processing at the MAC layer for preparing transmission (from the STS or BTS) and at the MAC layer for reception (at the BTS or STS).
- End-to-end delay: The total delay between a terminal in the subscriber network, to the ultimate service beyond the core network. This includes the transit delay.

Q 9) Describe the WAP protocol stack. What are the functions of the different layers in this protocol stack?

The Wireless Application Protocol (WAP) is a universal, open standard developed by the WAP Forum to provide mobile users of wireless phones and other wireless terminals such as pagers and personal digital assistants (PDAs) access to telephony and information services, including the Internet and the Web. WAP is designed to work with all wireless network technologies (e.g., GSM, CDMA, and TDMA).WAP is based on existing Internet standards, such as IP, XML, HTML, and HTTP, as much as possible. It also includes security facilities.

Architectural Overview:

The WAP Programming Model is based on three elements: the client, the gateway, and the original server. HTTP is used between the gateway and the original server to transfer content. The gateway acts as a proxy server for the wireless domain. Its processor(s) provide services that offload the limited capabilities of the hand-held, mobile, wireless terminals.

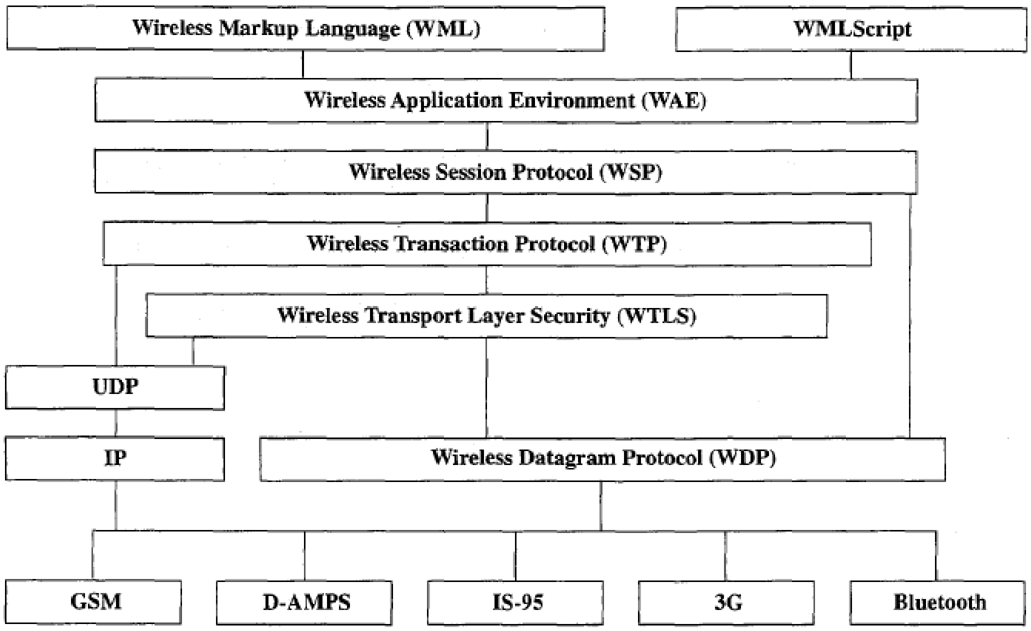

Wireless Markup Language (WML)
WMLScript
Wireless Application Environment (WAE)
Wireless Session Protocol (WSP)
Wireless Transaction Protocol (WTP)
Wireless Transport Layer Security (WTLS)
UDP
IP
Wireless Datagram Protocol (WDP)
GSM
D-AMPS
IS-95
3G
Bluetooth

Figure 12.8 WAP Protocol Stack

Wireless Markup Language(WML):

WML was designed to describe content and format for presenting data on devices with limited bandwidth, limited screen size, and limited user input capability. It is designed to work with telephone keypads, styluses, and other input devices common to mobile, wireless communication.

Important features of WML include the following:

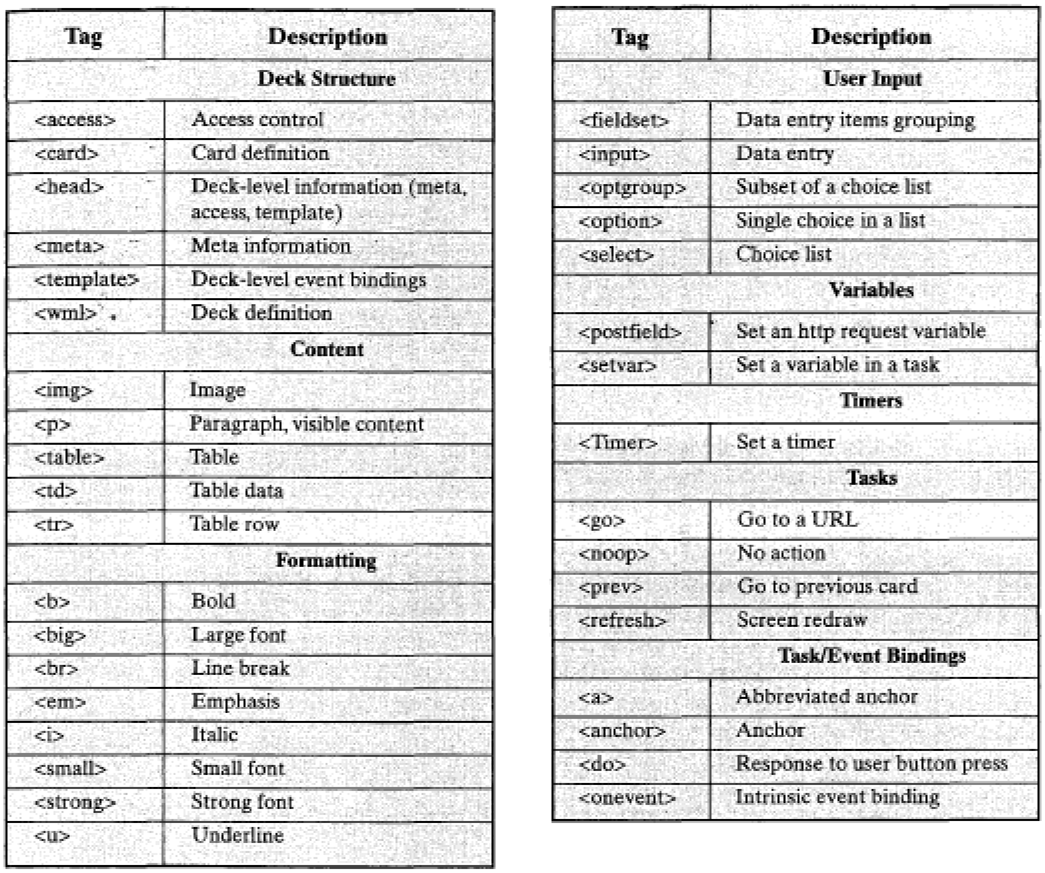
- Text and image support: Formatting and layout commands are provided for text and limited image capability.

- Deck/card organizational metaphor: WML documents are subdivided into small, well-defined units of user interaction called cards.
- Support for navigation among cards and decks: WML includes provisions for event handling, which is used for navigation or executing scripts.

<u>WML Script:</u>

WML Script is a scripting language with similarities to JavaScript. It is designed for defining script-type programs in a user device with limited processing power and memory.

WML Tags



Tag	Description
	Deck Structure
<access>	Access control
<card>	Card definition
<head>	Deck-level information (meta, access, template)
<meta>	Meta information
<template>	Deck-level event bindings
<wml>	Deck definition
	Content
<img>	Image
<p>	Paragraph, visible content
<table>	Table
<td>	Table data
<tr>	Table row
	Formatting
<b>	Bold
<big>	Large font
<br>	Line break
<em>	Emphasis
<i>	Italic
<small>	Small font
<strong>	Strong font
<u>	Underline

Tag	Description
	User Input
<fieldset>	Data entry items grouping
<input>	Data entry
<optgroup>	Subset of a choice list
<option>	Single choice in a list
<select>	Choice list
	Variables
<postfield>	Set an http request variable
<setvar>	Set a variable in a task
	Timers
<Timer>	Set a timer
	Tasks
<go>	Go to a URL
<noop>	No action
<prev>	Go to previous card
<refresh>	Screen redraw
	Task/Event Bindings
<a>	Abbreviated anchor
<anchor>	Anchor
<do>	Response to user button press
<onevent>	Intrinsic event binding

Key WML Script features include the following:

- <u>JavaScript-based scripting language:</u> WMLScript is a subset of JavaScript, with some extensions.
- <u>Procedural logic:</u> WMLScript adds the power of procedural logic to the Wireless Application Environment (WAE), discussed subsequently.
- <u>Event based:</u> WMLScript may be invoked in response to certain user or environmental events.

<u>Wireless Session Protocol:</u>

WSP provides applications with an interface for two session services. The connection oriented session service operates above the reliable transport protocol WTP, and the connectionless session service operates above the unreliable transport protocol WDP. In essence,WSP is based on HTTP with some additions and modifications to optimize its use over wireless channels.

WSP is a transaction-oriented protocol based on the concept of a request and a reply. Each WSP protocol data unit (PDU) consists of a body, which may contain WML, WMLScript, or images, and a header, which contains information about the data in the body and about the transaction. Session establishment involves the exchange of S-Connect primitives. A WSP user acting as a client (mobile node side of the transaction) requests a session with a WSP user acting as a server (Web Server) on a remote system by issuing an S-Connect.req to WSP.

Four parameters accompany the request:

- **Server address:** The peer with which the session is to be established.
- **Client address:** The originator of the session.
- **Client headers:** Contain attribute information that can be used for application level parameters to be communicated to the peer. This information is passed without modification by WSP and is not processed by WSP.
- **Requested capabilities:** A set of capabilities for this session requested by the Client.

Wireless Transaction Protocol:

WTP manages transactions by conveying requests and responses between a user agent (such as a WAP browser) and an application server for such activities as browsing and e-commerce transactions.

WTP includes the following features:

- Three classes of transaction service.
- Optional user-to-user reliability: WTP user triggers the confirmation of each received message.
- Optional out-of-band data on acknowledgments.
- PDU concatenation and delayed acknowledgment to reduce the number of messages sent.
- Asynchronous transactions.

Wireless Transport Layer Security:

WTLS provides security services between the mobile device (client) and the WAP gateway. WTLS is based on the industry-standard Transport Layer Security (TLS) Protocol, which is a refinement of the secure sockets layer (SSL). TLS is the standard security protocol used between Web browsers and Web servers.2 WTLS is more efficient that TLS, requiring fewer message exchanges.

WTLS provides the following features:

- Data integrity: Ensures that data sent between the client and the gateway are not modified, using message authentication
- Privacy: Ensures that the data cannot be read by a third party, using encryption

- Authentication: Establishes the authentication of the two parties, using digital certificates
- Denial-of-service protection: Detects and rejects messages that are replayed or not successfully verified.

Wireless Datagram Protocol:

WDP is used to adapt a higher-layer WAP protocol to the communication mechanism (called the bearer) used between the mobile node and the WAP gateway. Adaptation may include partitioning data into segments of appropriate size for the bearer and interfacing with the bearer network.

WDP Service-the WDP service is defined by two service primitives. The T-DUnitdata primitive provides a non-confirmed service with the following parameters:

- Source address: Address of the device making a request to the WDP layer
- Source port: Application address associated with the source address
- Destination address: Destination address for the data submitted to WDP
- Destination port: Application address associated with the destination address
- User data: User data from the next higher layer, submitted to WDP for transmission to the destination port.

Q 10) Why do you require spreading the spectrum? Explain the different methods of spreading the data and spectrum in a wireless environment.

Ans: 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 Figure 2.32, diagram i) shows an idealized narrowband 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 de-spread 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 band pass 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.

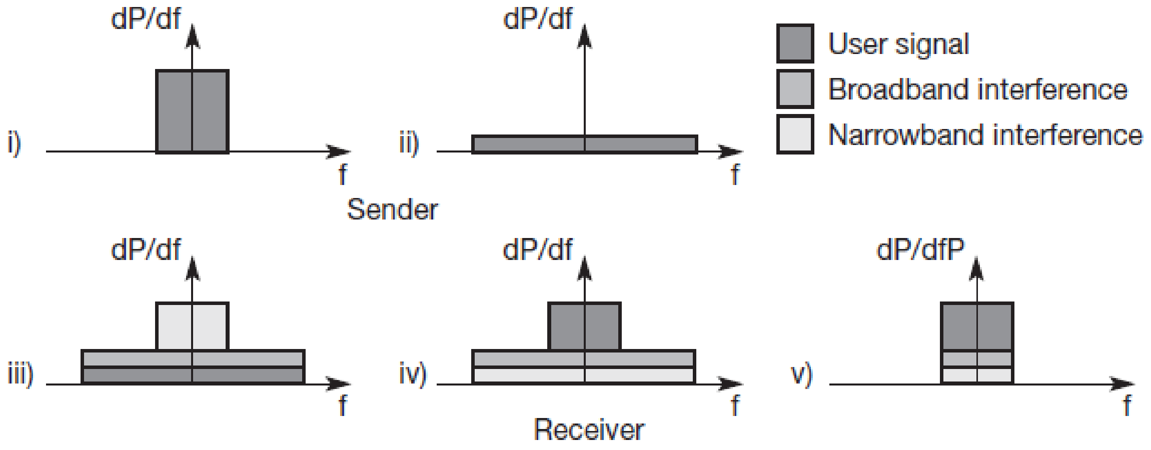


Fig 2.32 Spread spectrum: spreading and dispreading

Just as spread spectrum helps to deal with narrowband interference for a single channel, it can be used for several channels. Consider the situation shown in Figure 2.33. Six different channels use FDM for multiplexing, which means that each channel has its own narrow frequency band for transmission. Between each frequency band a guard space is needed to avoid adjacent channel interference.

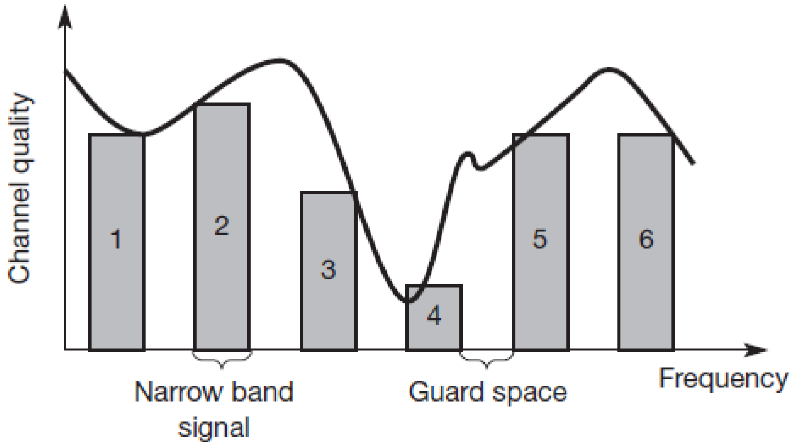


Figure 2.33 Narrowband interference without spread spectrum

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

1. Direct sequence spread spectrum:

Direct sequence spread spectrum (DSSS) systems take a user bit stream and perform an (XOR) with a so-called chipping sequence as shown in Figure 2.35. The example shows that the result is either the sequence 0110101 (if the user bit equals 0) or its complement 1001010 (if the user bit equals 1). While each user bit has a duration tb, the chipping sequence consists of smaller pulses, called chips, with a duration tc. If the chipping sequence is generated properly it appears as random noise: this sequence is also sometimes called pseudo-noise sequence. The spreading factor s = tb/tc determines the bandwidth of the resulting signal. If the original signal needs a bandwidth w, the resulting signal needs software after spreading.

While the spreading factor of the very simple example is only 7 (and the chipping sequence 0110101 is not very random), civil applications use spreading factors between 10 and 100, military applications use factors of up to 10,000. Wireless LANs complying with the standard IEEE 802.11 (see section 7.3) use, for example, the sequence 10110111000, a so-called Barker code, if implemented using DSSS. Barker codes exhibit a good robustness against interference and insensitivity to multi-path propagation. Other known Barker codes are 11, 110, 1110, 11101, 1110010, and 1111100110101 (Stallings, 2002). Up to now only the spreading has been explained. However, transmitters and receivers using DSSS need additional components as shown in the simplified block diagrams in Figure 2.36 and Figure 2.37.

The first step in a DSSS transmitter, Figure 2.36 is the spreading of the user data with the chipping sequence (digital modulation). The spread signal is then modulated with a radio carrier as explained in section 2.6 (radio modulation). Assuming for example a user signal with a bandwidth of 1 MHz. Spreading with the above 11-chip Barker code would result in a signal with 11 MHz bandwidth. The radio carrier then shifts this signal to the carrier frequency (e.g., 2.4 GHz in the ISM band). This signal is then transmitted.

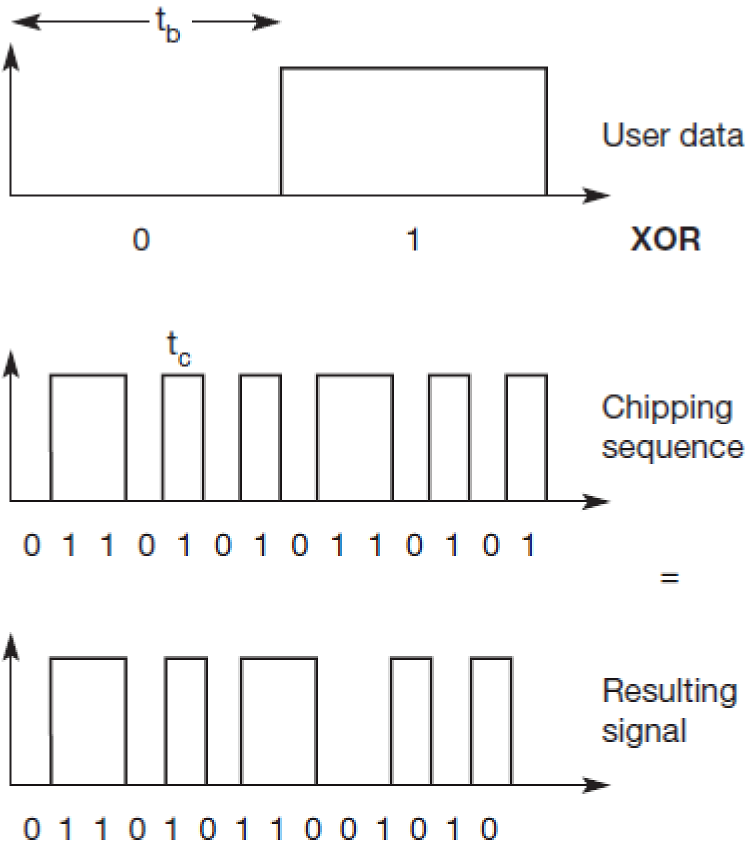


Figure 2.35 Spreading with DSSS

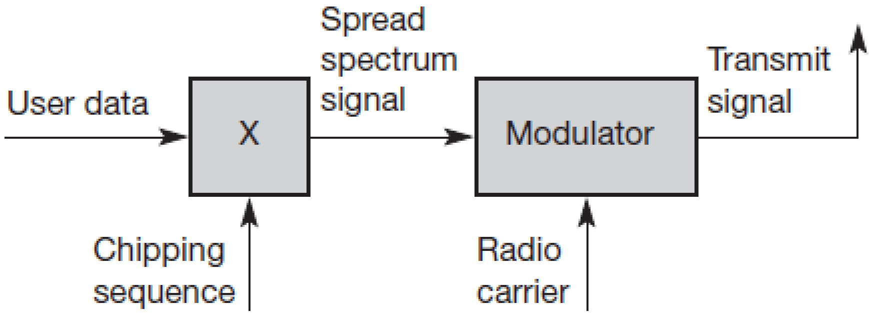


Figure 2.36 DSSS transmitter

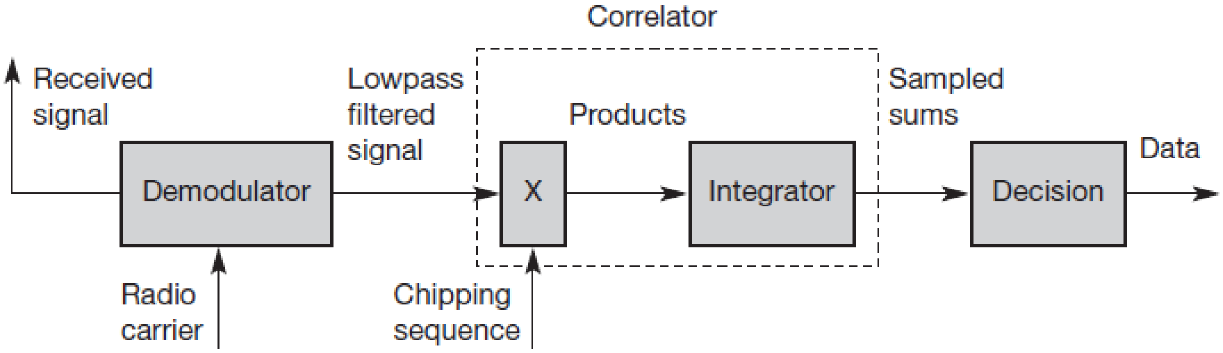


Figure 2.37 DSSS receiver

The DSSS receiver is more complex than the transmitter. The receiver only has to perform the inverse functions of the two transmitter modulation steps. However, noise and multi-path propagation require additional mechanisms to reconstruct the original data. The first step in the receiver involves demodulating the received signal. This is achieved using the same carrier as the transmitter reversing the modulation and results in a signal with approximately the same bandwidth as the original spread spectrum signal. Additional filtering can be applied to generate this signal. While demodulation is well known from ordinary radio receivers, the next steps constitute a real challenge for DSSS receivers, contributing to the complexity of the system.

The receiver has to know the original chipping sequence, i.e., the receiver basically generates the same pseudo random sequence as the transmitter. Sequences at the sender and receiver have to be precisely synchronized because the receiver calculates the product of a chip with the incoming signal. This comprises another XOR operation as explained in section 3.5, together with a medium access mechanism that relies on this scheme.

During a bit period, which also has to be derived via synchronization, an **integrator** adds all these products. Calculating the products of chips and signal, and adding the products in an integrator is also called correlation, the device a **correlator**. Finally, in each bit period a **decision unit** samples the sums generated by the integrator and decides if this sum represents a binary 1 or a 0. If transmitter and receiver are perfectly synchronized and the signal is not too distorted by noise or multi-path propagation, DSSS works perfectly well according to the simple scheme shown. Sending the user data 01 and applying the 11-chip Barker code 10110111000 results in the spread ‘signal’ 1011011100001001000111.

On the receiver side, this ‘signal’ is XORed bit-wise after demodulation with the same Barker code as chipping sequence. This results in the sum of products equal to 0 for the first bit and to 11 for the second bit. The decision unit can now map the first sum (=0) to a binary 0, the second sum (=11) to a binary 1 – this constitutes the original user data. In real life, however, the situation is somewhat more complex. Assume that the demodulated signal shows some distortion, e.g., 101**0**01**0**100001**1**01000111.

The sum of products for the first bit would be 2, 10 for the second bit. Still, the decision unit can map, e.g., sums less than 4 to a binary 0 and sums larger than 7 to a binary 1. However, it is important to stay synchronized with the transmitter of a signal. But what happens in case of multi-path propagation? Then several paths with different delays exist between a transmitter and a receiver.

Additionally, the different paths may have different path losses. In this case, using so-called rake receivers provides a possible solution. A rake receiver uses n correlators for the n strongest paths. Each correlator is synchronized to the transmitter plus the delay on that specific path. As soon as the receiver detects a new path which is stronger than the currently weakest path, it assigns this new path to the correlator with the weakest path. The output of the correlators are then combined and fed into the decision unit. Rake receivers can even take advantage of the multi-path propagation by combining the different paths in a constructive way (Viterbi, 1995).

2. Frequency hopping spread spectrum:

For frequency hopping spread spectrum (FHSS) systems, the total available bandwidth is split into many channels of smaller bandwidth plus guard spaces between the channels. Transmitter and receiver stay on one of these channels for a certain time and then hop to another channel. This system implements FDM and TDM. The pattern of channel usage is called the hopping sequence, the time spend on a channel with a certain frequency is called the dwell time.
FHSS comes in two variants, slow and fast hopping (see Figure 2.38).

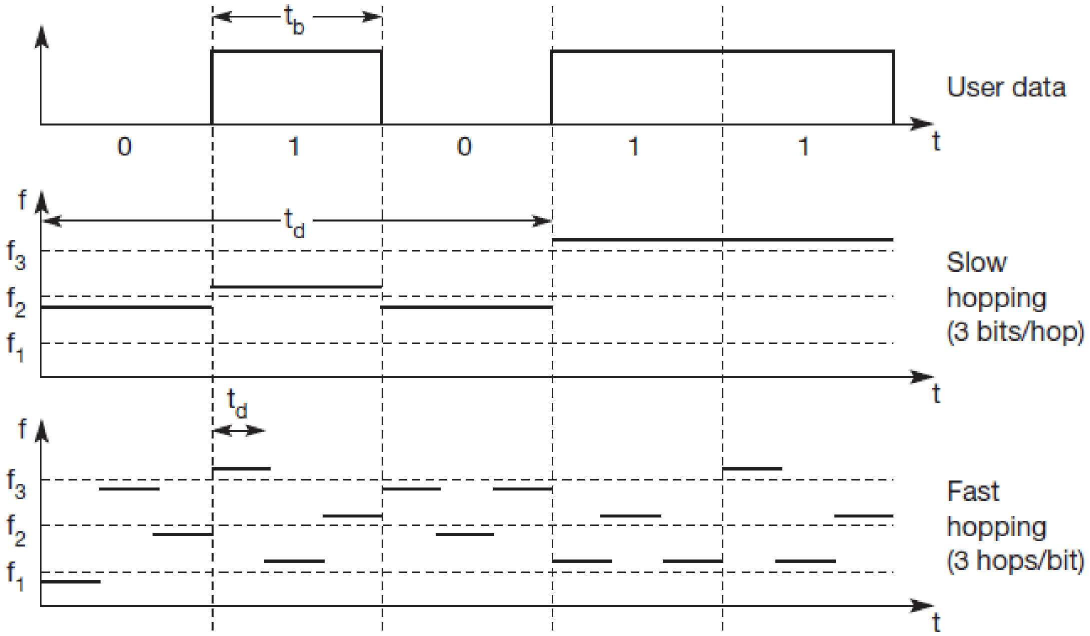


Figure 2.38 Slow and fast frequency hopping

In slow hopping, the transmitter uses one frequency for several bit periods. Figure 2.38 shows five user bits with a bit period tb. Performing slow hopping, the transmitter uses the frequency f2 for transmitting the first three bits during the dwell time td. Then, the transmitter hops to the next frequency f3. Slow hopping systems are typically cheaper and have relaxed tolerances, but they are not as immune to narrowband interference as fast hopping systems. Slow frequency hopping is an option for GSM. For fast hopping systems, the transmitter changes the frequency several times during the transmission of a single bit.

In the example of Figure 2.38, the transmitter hops three times during a bit period. Fast hopping systems are more complex to implement because the transmitter and receiver have to stay synchronized within smaller tolerances to perform hopping at more or less the same points in time. However, these systems are much better at overcoming the effects of narrowband interference and frequency selective fading as they only stick to one frequency for a very short time. Another example of an FHSS system is Bluetooth, which is presented in section 7.5. Bluetooth performs 1,600 hops per second and uses 79 hop carriers equally spaced with 1 MHz in the 2.4 GHz ISM band. Figures 2.39 and 2.40 show simplified block diagrams of FHSS transmitters and receivers respectively.

The first step in an FHSS transmitter is the modulation of user data according to one of the digital-to-analog modulation schemes, e.g., FSK or BPSK, as discussed in section 2.6. This results in a narrowband signal, if FSK is used with a frequency f0 for a binary 0 and f1 for a binary 1. In the next step, frequency hopping is performed, based on a hopping sequence. The hopping sequence is fed into a frequency synthesizer generating the carrier frequencies fi. A second modulation uses the modulated narrowband signal and the carrier frequency to generate a new spread signal with frequency of fi+f0 for a 0 and fi+f1 for a 1 respectively.

If different FHSS transmitters use hopping sequences that never overlap, i.e., if two transmitters never use the same frequency fi at the same time, then these two transmissions do not interfere. This requires the coordination of all transmitters and their hopping sequences. As for DSSS systems, pseudo-random hopping sequences can also be used without coordination. These sequences only have to fulfill certain properties to keep interference minimal.4 Two or more transmitters may choose the same frequency for a hop, but dwell time is short for fast hopping systems, so interference is minimal.

The receiver of an FHSS system has to know the hopping sequence and must stay synchronized. It then performs the inverse operations of the modulation to reconstruct user data. Several filters are also needed (these are not shown in the simplified diagram in Figure 2.40).

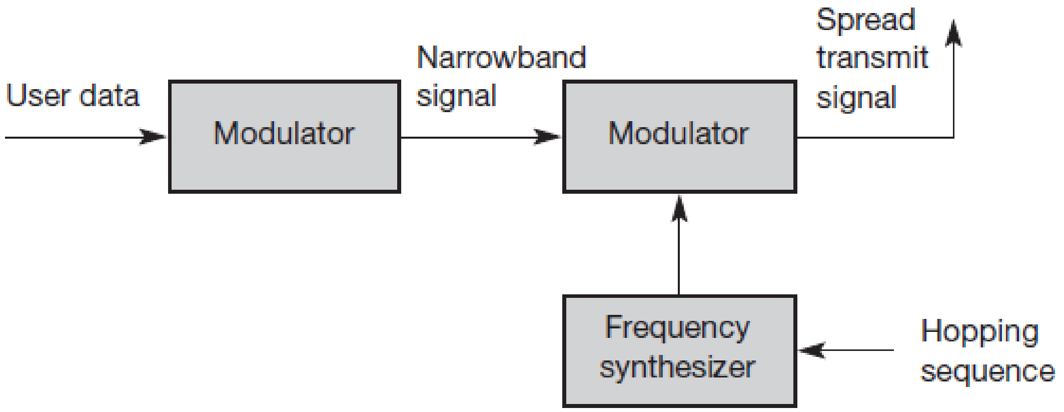


Figure 2.39 FHSS transmitter

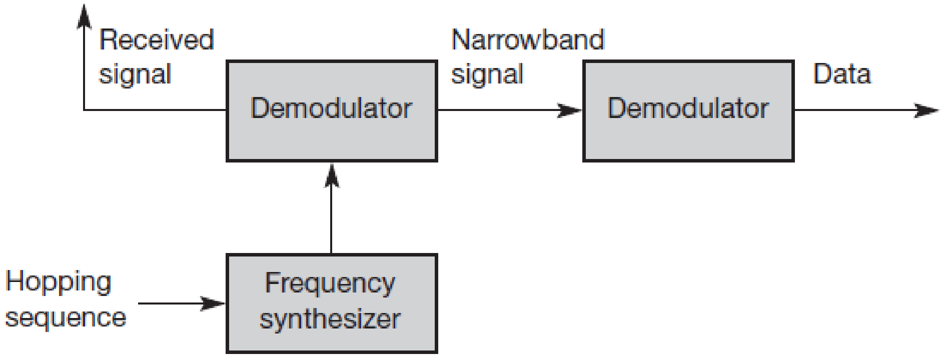


Figure 2.40 FHSS receiver

Q 11) What is the difference between GSM and GPRS? Explain the architecture of GPRS.

Ans: The GPRS architecture introduces two new network elements, which are called GPRS support nodes (GSN) and are in fact routers. All GSNs are integrated into the standard GSM architecture, and many new interfaces have been defined (see Figure 4.16). The gateway GPRS support node (GGSN) is the interworking unit between the GPRS network and external packet data networks (PDN). This node contains routing information for GPRS users, performs address conversion, and tunnels data to a user via encapsulation. The GGSN is connected to external networks (e.g., IP or X.25) via the Gi interface and transfers packets to the SGSN via an IP-based GPRS backbone network (Gn interface).

The other new element is the serving GPRS support node (SGSN) which supports the MS via the Gb interface. The SGSN, for example, requests user addresses from the GPRS register (GR), keeps track of the individual MSs' location, is responsible for collecting billing information (e.g., counting bytes), and performs several security functions such as access control. The SGSN is connected to a BSC via frame relay and is basically on the same hierarchy level as an MSC. The GR, which is typically a part of the HLR, stores all GPRS-relevant data. GGSNs and SGSNs can be compared with home and foreign agents, respectively, in a mobile IP network.

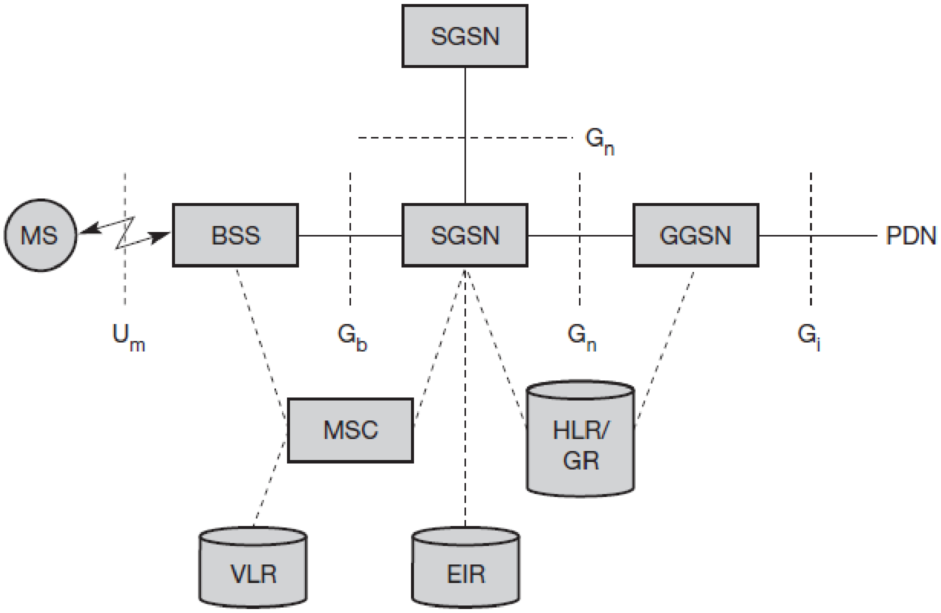


Figure 4.16 GPRS architecture reference model

As shown in Figure 4.16, packet data is transmitted from a PDN, via the GGSN and SGSN directly to the BSS and finally to the MS. The MSC, which is responsible for data transport in the traditional circuit-switched GSM, is only used for signaling in the GPRS scenario. Additional interfaces to further network elements and other PLMNs can be found in ETSI (1998b). Before sending any data over the GPRS network, an MS must attach to it, following the procedures of the mobility management. The attachment procedure includes assigning a temporal identifier, called a temporary logical link identity (TLLI), and a ciphering key sequence number (CKSN) for data encryption.

For each MS, a GPRS context is set up and stored in the MS and in the corresponding SGSN. This context comprises the status of the MS (which can be ready, idle, or standby; ETSI, 1998b), the CKSN, a flag indicating if compression is used, and routing data (TLLI, the routing area RA, a cell identifier, and a packet data channel, PDCH, identifier). Besides attaching and detaching, mobility management also comprises functions for authentication, location management, and ciphering (here, the scope of ciphering lies between MS and SGSN, which is more than in standard GSM). In idle mode an MS is not reachable and all context is deleted. In the standby state only movement across routing areas is updated to the SGSN but not changes of the cell. Permanent updating would waste battery power, no updating would require system-wide paging. The update procedure in standby mode is a compromise. Only in the ready state every movement of the MS is indicated to the SGSN.

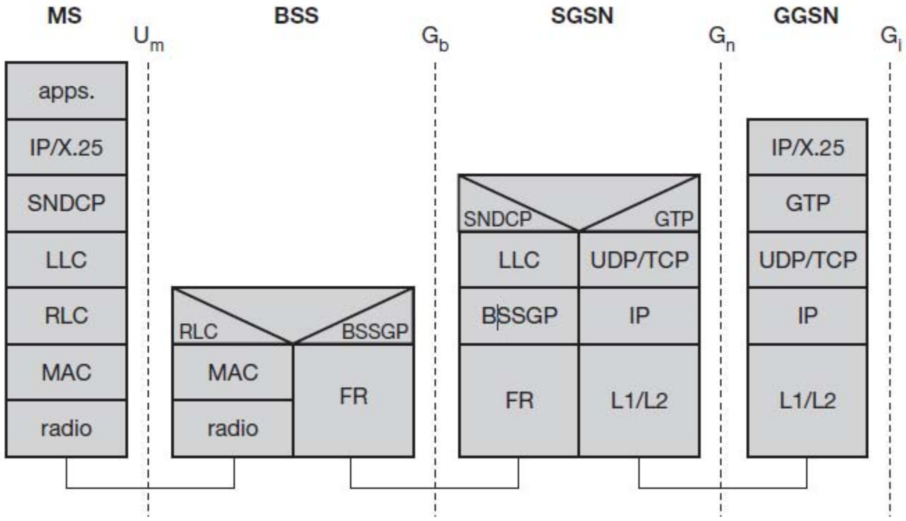


Figure 4.17 GPRS transmission plane protocol reference model

Figure 4.17 shows the protocol architecture of the transmission plane for GPRS. Architectures for the signaling planes can be found in ETSI (1998b). All data within the GPRS backbone, i.e., between the GSNs, is transferred using the GPRS tunnelling protocol (GTP). GTP can use two different transport protocols, either the reliable TCP (needed for reliable transfer of X.25 packets) or the non-reliable UDP (used for IP packets). The network protocol for the GPRS backbone is IP (using any lower layers).

To adapt to the different characteristics of the underlying networks, the subnetwork dependent convergence protocol (SNDCP) is used between an SGSN and the MS. On top of

SNDCP and GTP, user packet data is tunneled from the MS to the GGSN and vice versa. To achieve a high reliability of packet transfer between SGSN and MS, a special LLC is used, which comprises ARQ and FEC mechanisms for PTP (and later PTM) services. A base station subsystem GPRS protocol (BSSGP) is used to convey routing and QoS-related information between the BSS and SGSN. BSSGP does notperform error correction and works on top of a frame relay (FR) network.

Finally, radio link dependent protocols are needed to transfer data over the Um interface. The radio link protocol (RLC) provides a reliable link, while the MAC controls access with signaling procedures for the radio channel and the mapping of LLC frames onto the GSM physical channels. The radio interface at Um needed for GPRS does not require fundamental changes compared to standard GSM (Brasche, 1997), (ETSI, 1998d). However, several new logical channels and their mapping onto physical resources have been defined. For example, one MS can allocate up to eight packet data traffic channels (PDTCHs). Capacity can be allocated on demand and shared between circuit-switched channels and GPRS.

This allocation can be done dynamically with load supervision or alternatively, capacity can be pre-allocated. A very important factor for any application working end-to-end is that it does not ‘notice’ any details from the GSM/GPRS-related infrastructure. The application uses, e.g., TCP on top of IP, IP packets are tunneled to the GGSN, which forwards them into the PDN. All PDNs forward their packets for a GPRS user to the GGSN, the GGSN asks the current SGSN for tunnel parameters, and forwards the packets via SGSN to the MS. Although MSs using GPRS may be considered as part of the internet, one should know that operators typically perform an address translation in the GGSN using NAT.

All MSs are assigned private IP addresses which are then translated into global addresses at the GGSN. The advantage of this approach is the inherent protection of MSs from attacks (the subscriber typically has to pay for traffic even if it originates from an attack!) – private addresses are not routed through the internet so it is not possible to reach an MS from the internet. This is also a disadvantage if an MS wants to offer a service using a fixed, globally visible IP address. This is difficult with IPv4 and NAT and it will be interesting to see how IPv6 is used for this purpose (while still protecting the MSs from outside attacks as air traffic is expensive).

GSM	GPRS
1. GSM is Global System for Mobile Communications.	1. GPRS is General Packet Radio Service.
2. GSM is a wireless platform that uses radio frequencies. It has been designed for speech services and uses circuit switched transmission.	2. GPRS is a separate packet data network which provides a packet base platform both for the data transfer and signaling.
3. It is one of the leading digital cellular systems.	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.	6. GPRS is a mobile data service available to users of GSM mobile phones.
7. GSM uses a combination of Frequency Division Multiple Access (FDMA) and Time Division Multiple Access(TDMA).	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.

Q 12) Discuss the MAC layer of the IEEE 802.11.

Ans: The IEEE 802.11 MAC layer covers three functional areas: reliable data delivery, medium access control and security.

Reliable Data Delivery:

A wireless LAN using the IEEE 802.11 physical and MAC layers is subject to considerable unreliability. Noise, interference, and other propagation effects result in the loss of a significant number of frames. Even with error-correction codes, a number of MAC frames may not successfully be received.

IEEE 802.11 includes a frame exchange protocol. When a station receives a data frame from another station, it returns an acknowledgement (ACK) frame to the source station. This exchange is treated as an atomic unit, not to be interrupted by a transmission from any other station.

Medium Access Control:

The end result for 802.11 is a MAC algorithm called DFWMAC (distributed foundation wireless MAC) that provides a distributed access control mechanism with an optional centralized control built on top of that. In the figure, the lower sublayer of the MAC layer is the distributed coordination function (DCF). DCF uses a contention algorithm to provide access to all traffic. Ordinary asynchronous traffic directly uses DCF. The point coordination function (PCF) is a centralized MAC algorithm used to provide contention-free service. PCF is built on top of DCF and exploits features of DCF to assure access for its users.

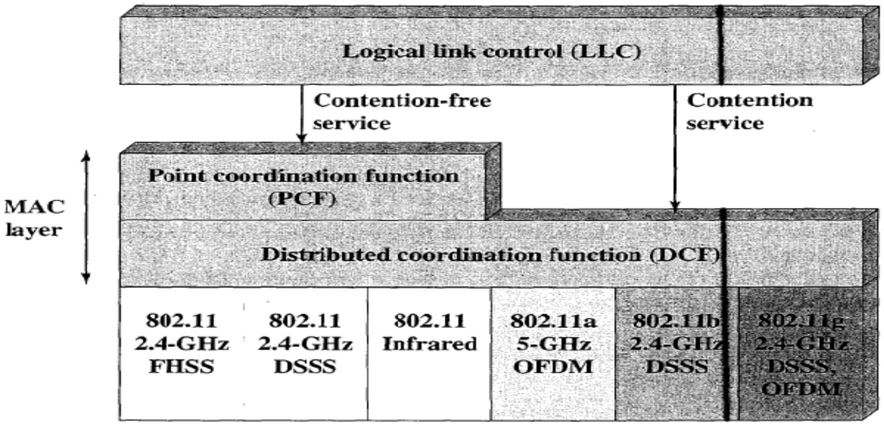
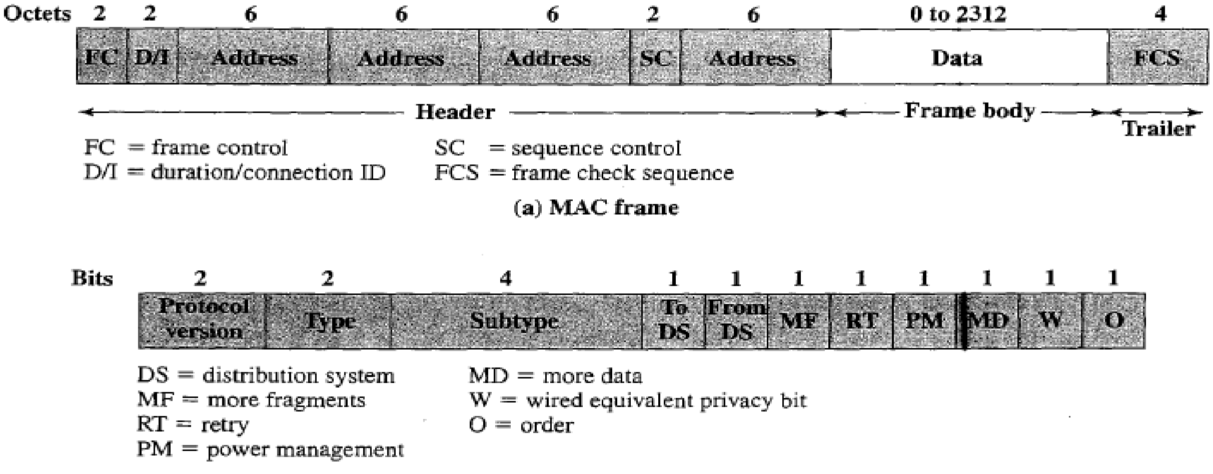


Figure 14.5 IEEE 802.11 Protocol Architecture

The DCF sublayer makes use if a simple CSMA algorithm. If a station has a MAC frame to transmit, it listens to the medium. If the medium is idle, the station may transmit; otherwise the station must wait until the current transmission is complete before transmitting.

PCF is an alternative access method implemented on top of the DCF. The operation consists of polling by the centralized polling master. The point coordinator makes use of PIFS when issuing polls. Because PIFS is smaller than DIFS, the point coordinator can seize the medium and lock out all asynchronous traffic while it issues polls and receives responses.

MAC Frame:



(a) MAC frame

(b) Frame control field

Figure 14.8 IEEE 802.11 MAC Frame Format

The above frame format shows the IEEE 802.11 frame format when no security features are used. This general format is used for all data and control frames. The fields are as follows:

- Frame Control: Indicates the type of frame and provides control information.
- Duration/Connection ID: If used as a duration field, indicates the time (microseconds) the channel will be allocated for successful transmission of a MAC frame. In some control frames, this field contains an association, or connection identifier.
- Addresses: The number and meaning of the 48-bit address fields depend on the context. The transmitter address and receiver address are the MAC addresses of the stations joined to the BSS that are transmitting and receiving frames over the wireless LAN.
- Sequence Control: Contains a 4-bit fragment number subfield used for fragmentation and reassembly, and a 12-bit sequence number used to number frames sent between a given transmitter and receiver.
- Frame Body: Contains an MSDU or a fragment of an MSDU. The MSDU is a LLC protocol data unit or MAC control information.
- Frame Check Sequence: A 32-bit cyclic redundancy check.

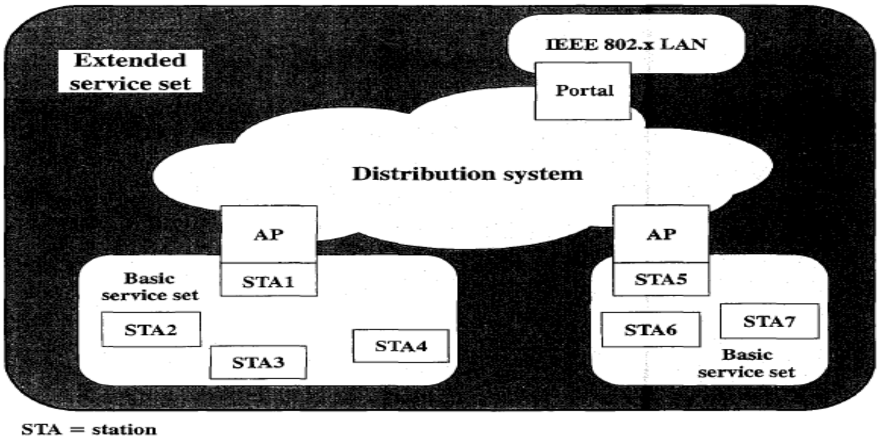
The frame control field consists of the following fields:

- Protocol version: 802.11 version, currently version 0.
- Type: Identifies the frame as control, management, or data.
- Subtype: Further identifies the function of frame.
- To DS: The MAC coordination sets this bit to 1 in a frame destined to the distribution system.
- From DS: The MAC coordination sets this bit to 1 in a frame leaving the distribution system.
- More Fragments: Set to 1 if more fragments follow this one.
- Retry: Set to 1 if this is a retransmission of a previous frame.

This is the MAC layer of the IEEE 802.11.

Q 13) Explain in detail IEEE 802.11 system architecture and discuss the services provided by 802.11.

IEEE 802.11 Architecture:



STA = station

Figure 14.4 IEEE 802.11 Architecture

The smallest building block of a wireless LAN is a basic service set (BSS), which consists of some number of stations executing the same MAC protocol and competing for access to the same shared wireless medium. A BSS may be isolated or connect to a backbone distribution system (DS) through an access point (AP). The AP functions as a bridge and relay point. In a BSS, client stations do not communicate directly with one another. Rather, if one station in the BSS wants to communicate with another station in the same BSS, the MAC frame is first sent from the originating station to the AP, then from the AP to the destination station. Similarly, a MAC frame from a station in the BSS to a remote station is sent from the local station to the AP and then relayed by the AP over the DS on its way to the destination station.

When all the stations in the BSS are mobile stations, with no connection to other BSSs, the BSS is called the independent BSS (IBSS). An IBSS is typically an ad hoc network. An extended service set (ESS) consists of two or more basic service sets interconnected by a distribution system. Typically, the distribution system is a wired backbone LAN but can be any communications network. To integrate the IEEE 802.11 architecture with a traditional wired LAN, a portal is used. The portal logic is implemented in a device, such as a bridge or router, that is part of the wired LAN and is attached to the DS.

IEEE 802.11 Services:

IEEE 802.11 defines nine services that need to be provided by the wireless LAN to provide functionality equivalent to that which is inherent to wired LANs. The table below lists these services and indicates two ways of categorizing them – the service provider and function for which the service is used.

Service	**Provider**	**Used to Support**
Association	Distribution system	MSDU delivery
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Disassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU Delivery	Station	MSDU delivery
Privacy	Station	LAN access and security
Reassociation	Distribution system	MSDU delivery

Table: IEEE 802.11 Services

The various services designed to clarify the operation of IEEE 802.11 ESS network are as follows:

Distribution of Messages within a DS:

Distribution is the primary service used by stations to exchange MAC frames when the frame must transverse the DS to get from a station in one BSS to a station in another BSS.
The integration service enables transfer of data between a station on an IEEE 802.11 LAN and a station on an IEEE 802.x integrated LAN.

Association-Related Services:

For the distribution service to function for transferring MSDUs, it requires information about the station within an ESS, which is provided by the association-related services. Before the distribution service can deliver data to or accept data from a station, that station must be associated based on the concept of mobility- No transition, BSS transition, ESS transition.

Three services relate to this requirement as follows:

- Association: Establishes an initial association with station and AP.
- Reassociation: Enables an established association to be transferred from one AP to another, allowing a mobile station to move from one BSS to another.
- Disassociation: A notification from either a station or an AP that an existing association is terminated.

Access and Privacy Services:

We can ensure access and privacy using three services as follows:

- Authentication: Used to establish identity of stations to each other.
- Deauthentication: This service is invoked whenever the existing authentication is to be terminated.
- Privacy: Used to prevent contents of messages from being read by other than the intended recipient. The standard provides for the optional use of encryption to assure privacy.

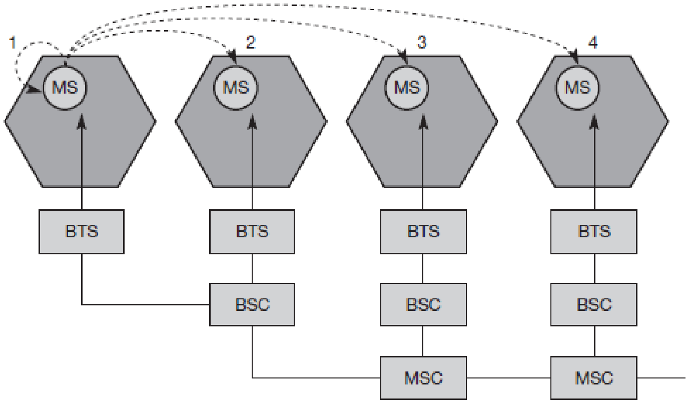
Q.14) Give reasons for handover in GSM and the problem associated with it. What are the typical steps for handover, what types of handovers can occur?

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:



Above fig. explains all types of handovers which are listed above.

Q 15) Explain CDMA. List Advantages of CDMA over FDMA

Ans:

Code Division Multiple access (CDMA) system use the code with the certain characteristics can be applied to the transmission to enable the use of Code Division Multiplexing (CDM) to separate different users in code space and to enable access to a shared medium without interference. The main problem is how to find "good" code and how to separate the signal from noise generated by other signals and the environment.

A code for a certain user should have a good **autocorrelation** and should be **orthogonal** to other codes. Two vectors are called orthogonal if their internal product is 0, as is the case for the two vectors (2,5,0) and (0,0,17) : (2,5,0) * (0,0,17) =0+0+0+0=0.But also vectors like(3,-2,4)and (-2,3,3)are orthogonal (3,-2,4)*(-2,3,3)= -6-6+12=0. Orthogonality cannot be guaranteed for initially orthogonal codes.

After this quick introduction to orthogonality and autocorrelation the following example explains the basic functions of CDMA before it applies to signals.

- Two Senders A and B want to send data . CDMA assigned the following unique orthogonal key sequence: key Ak=010011 for sender A, Key Bk =110101 for sender B. Sender A wants to send Bit Ad =1,Sender B sends Bd =0. To illustrate this eg. Let us Assume that we code a binary 0 as -1,A binary 1 as +1. We can then apply standard addition and multiplication rule.
- Both Senders spread their signals using their key as chipping sequence. In reality, part of much longer chipping sequence are applied to signals bits for spreading. Sender A sends the signals As =Ad*Ak=+1*(-1,+1,-1,-1,+1,+1)=(-1,+1,-1,-1,+1,+1). Sender B does the same with the data to spread the signal with the code: Bs=Bd*Bk=-1*(+1,+1,-1,+1,-1,+1)=(-1,-1,+1,-1,+1,-1).
- Both the signal are transmitted at the same time using the same frequency , So, The Signals superimpose in space. Discounting interace from other senders and environmental noise from this simple eg. ,and assuming that signals have the same strength at receiver, the following signals C is receive at receiver end :C=As+Bs=(-2,0,0,-2,+2,0).
- The receiver wants to receive the data from sender A and ,therefore,tunes into the code A, that is applies A's is code for dispreading:C*Ak=(-2,0,0,-2,+2,0)* (-1,+1,-1,-1,+1,+1)=2+0+0+2+2+0=6. As the result is much longer than 0, the receiver detect the binary 1.Tuning into the B that is B's code gives C*Bk=(-2,0,0,-2,+2,0)* (+1,+1,-1,+1,-1,+1)=-2+0+0-2-2+0=-6 the result is negative so 0 has been detected

Advantages of CDMA over FDMA

Approach	**FDMA**	**CDMA**
Idea	Segment frequency band into disjoint Sub bands	Spread the spectrum using Orthogonal codes
Terminals	Every terminal has its own frequency, uninterrupted	All terminals can be active at the same place at the same moment, uninterrupted
Signal Separation	Filtering in the frequency domain	Code plus special receivers
Advantages	Simple , establish, Robust	Flexible, less planning need , soft hand over
Disadvantages	Inflexible, Frequencies are Scarce resource	Complex Receivers, need more complicated power control for senders

Q17 Explain the J2ME architecture. List the limitation of J2ME. What profiles are supported by CLDC configuration?

Ans:

J2ME Architecture:

The J2ME architecture comprises three software layers. The first layer is the configuration layer that includes the Java Virtual Machine (JVM), which directly interacts with the native operating system. The configuration layer also handles interactions between the profile and the JVM. The second layer is the profile layer, which consists of the minimum set of application programming interfaces (APIs) for the small computing device. The third layer is the Mobile Information Device Profile (MIDP). The MIDP layer contains Java APIs for user network connections, persistence storage, and the user interface. It also has access to CLDC libraries and MIDP libraries.

A small computing device has two components supplied by the original equipment manufacturer (OEM). These are classes and applications. OEM classes are used by the MIDP to access device-specific features such as sending and receiving messages and accessing device-specific persistent data. OEM applications are programs provided by the OEM, such as an address book. OEM applications can be accessed by the MIDP.

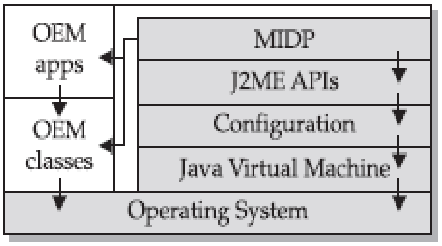


Figure 3-1. *Layers of the J2ME architecture*

Some of the limitations of J2ME are:

- Some J2SE applications require classes that are not available in J2ME.
- Java applications won't run in the J2ME environment without requiring modification to the code.
- . Devices that use the **CDC configuration** use the full **Java Virtual Machine** implementation, while devices that use the **CLDC configuration** use the **Kjava Virtual Machine** implementation.
- MIDlets are controlled by **application management software (AMS)**. So we cant invoke a MIDLET like a J2SE Application.

Mobile Information Device Profile and PDA Profile are supported by CLDC configuration.

- Mobile Information Device Profile:
  The Mobile Information Device Profile (MIDP) is used with the CLDC configuration and contains classes that provide local storage, a user interface, and networking capabilities to an application that runs on a mobile computing device such as Palm OS devices. MIDP is used with wireless Java applications.
- PDA Profile:
  The PDA Profile (PDAP) is used with the CLDC configuration and contains classes that utilize sophisticated resources found on personal digital assistants. These features include better displays and larger memory than similar resources found on MIDP mobile devices.

Q 18) What is WAP? Describe WML and WDP.

Ans: Wireless Application Protocol (**WAP**) is a technical standard for accessing information over a mobile wireless network. A WAP browser is a web browser for mobile devices such as mobile phones (called "cellular phones" in some countries) that uses the protocol.

Before the introduction of WAP, mobile service providers had limited opportunities to offer interactive data services, but needed interactivity to support Internet and Web applications such as:

- Email by mobile phone
- Tracking of stock-market prices
- Sports results
- News headlines
- Music downloads

The WAP standard described a protocol suite allowing the interoperability of WAP equipment and software with different network technologies, such as GSM and IS-95 (also known as CDMA).

```
.+------------------------------------------+
 .| Wireless Application Environment (WAE)   |
 .+------------------------------------------+  \
 .| Wireless Session Protocol (WSP)          |   |
 .+------------------------------------------+   |
 .| Wireless Transaction Protocol (WTP)      |   | WAP
 .+------------------------------------------+   | protocol
 .| Wireless Transport Layer Security (WTLS) |   | suite
 .+------------------------------------------+   |
 .| Wireless Datagram Protocol (WDP)         |   |
 .+------------------------------------------+  /
 .|     *** Any Wireless Data Network ***    |
 .+------------------------------------------+
```

The bottom-most protocol in the suite, the WAP Datagram Protocol (WDP), functions as an adaptation layer that makes every data network look a bit like UDP to the upper layers by providing unreliable transport of data with two 16-bit port numbers (origin and destination). All the upper layers view WDP as one and the same protocol, which has several "technical realizations" on top of other "data bearers" such as SMS, USSD, etc. On native IP bearers such as GPRS, UMTS packet-radio service, or PPP on top of a circuit-switched data connection, WDP is in fact exactly UDP.

WTLS, an optional layer, provides a public-key cryptography-based security mechanism similar to TLS.

WTP provides transaction support (reliable request/response) adapted to the wireless world. WTP supports more effectively than TCP the problem of packet loss, which occurs commonly in 2G wireless technologies in most radio conditions, but is misinterpreted by TCP as network congestion.

Finally, one can think of WSP initially as a compressed version of HTTP.

This protocol suite allows a terminal to transmit requests that have an HTTP or HTTPS equivalent to a WAP gateway; the gateway translates requests into plain HTTP.

WML

Wireless Markup Language, based on XML, is a markup language intended for devices that implement the Wireless Application Protocol (WAP) specification, such as mobile phones. It provides navigational support, data input, hyperlinks, text and image presentation, and forms, much like HTML (HyperText Markup Language). It preceded the use of other markup languages now used with WAP, such as HTML itself, and XHTML (which are gaining in popularity as processing power in mobile devices increases).

A WML document is known as a “deck”. Data in the deck is structured into one or more “cards” (pages) – each of which represents a single interaction with the user. The introduction of the terms "deck" and "card" into the internet and mobile phone communities was a result of the user interface software and its interaction with wireless communications services having to comply with the requirements of the laws of two or more nations.

WML decks are stored on an ordinary web server configured to serve the text/vnd.wap.wml MIME type in addition to plain HTML and variants. The WML cards when requested by a device are accessed by a bridge WAP gateway, which sits between mobile devices and the World Wide Web, passing pages from one to the other much like a proxy. The gateways send the WML pages on in a form suitable for mobile device reception (WAP Binary XML). This process is hidden from the phone, so it may access the page in the same way as a browser accesses HTML, using a URL (for example, http://example.com/foo.wml). (Provided the mobile phone operator has not specifically locked the phone to prevent access of user-specified URLs.)

WDP

These three protocols can be thought of as "glue layers" in WAP:

- Wireless Transaction Protocol (WTP)
- Wireless Transaction Layer Security (WTLS)
- Wireless Datagram Protocol (WDP)

WDP implements an abstraction layer to lower-level network protocols; it performs functions similar to UDP. WDP is the bottom layer of the WAP stack, but it does not implement physical or data link capability. To build a complete network service, the WAP stack must be implemented on some low-level *legacy* interface not technically part of the model. These interfaces, called *bearer services* or *bearers*, can be IP-based or non-IP based.

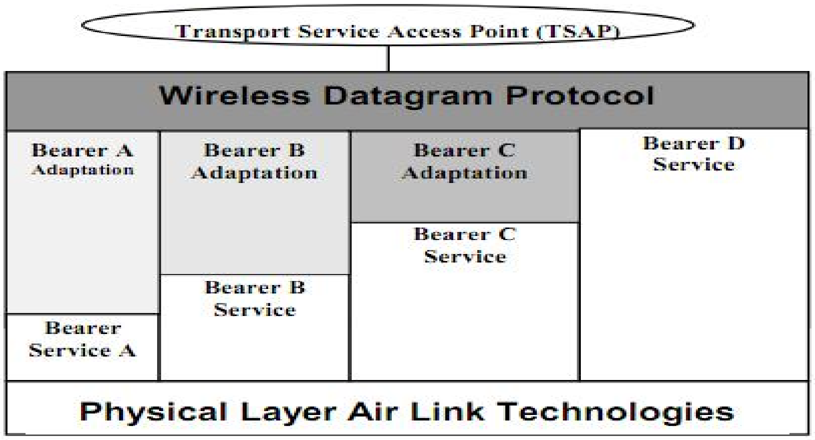


Fig WDP

WDP offers a consistent service at the Transport Service Access Point to the upper layer protocol of WAP. This consistency of service allows for applications to operate transparently over different available bearer services. The varying heights of each of the bearer services shown in figure illustrates the difference in functions provided by the bearers and thus the difference in WDP protocol necessary to operate over those bearers to maintain the same service offering at the Transport Service Access Point is accomplished by a bearer adaptation. WDP can be mapped onto different bearers, with different characteristics. In order to optimise the protocol with respect to memory usage and radio transmission efficiency, the protocol performance over each bearer may vary. However, the WDP service and service primitives will remain the same, providing a consistent interface to the higher layers.

Q 19) List the benefits of spread spectrum. Describe frequency hopping spread spectrum technique?

Ans:

An increasing form of communication is known as spread spectrum which is used to transmit either analog or digital data using an analog signal.

The essential idea of spread spectrum technique is to spread the information signal over a wider bandwidth to make jamming and interception more difficult.

The benefits of spread spectrum are as follows:

- We can gain immunity from various kinds of noise and multipath distortion. The earliest applications of spread spectrum were military, where it was used for its immunity to jamming.
- It can also be used for hiding and encrypting signals. Only the recipient who knows the spreading code can recover the encoded information.
- Several users can independently use the same higher bandwidth with very little interference. This property is used in cellular telephony applications, with a technique known as code division multiplexing (CDM) or code division multiple access (CDMA).

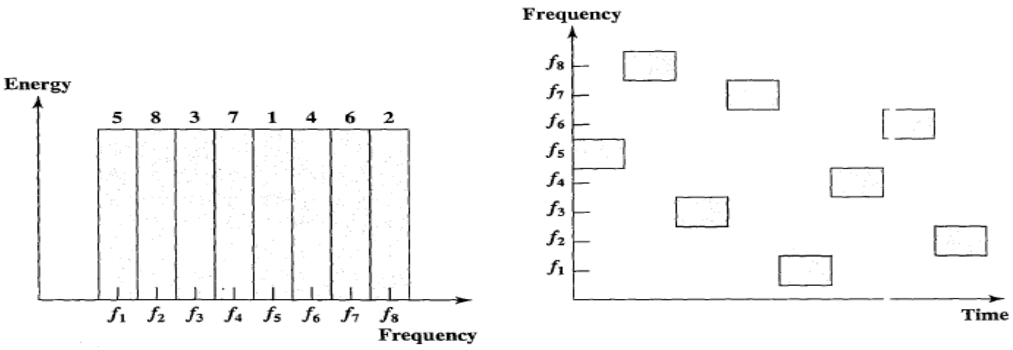
Frequency Hopping Spread Spectrum (fhss):

In this type, the signal is broadcast over a random series of radio frequencies, hopping from frequency to frequency at fixed intervals.

A receiver hopping between the frequencies in synchronization with the transmitter picks up the message.

FHSS basic approach:

- Number of channels allocated for FH signal
- 2k carrier frequencies, one for each channel
- The spacing between carrier frequencies and hence the channel width related to input bandwidth.
- The transmitter operates in one channel at a time for a fixed interval. During this interval, some number of bits is transmitted using some encoding scheme.
- The sequence of channel used is dedicated by a spreading code.
- Both the transmitter and receiver use the same code to tune into a sequence of channels in synchronizations

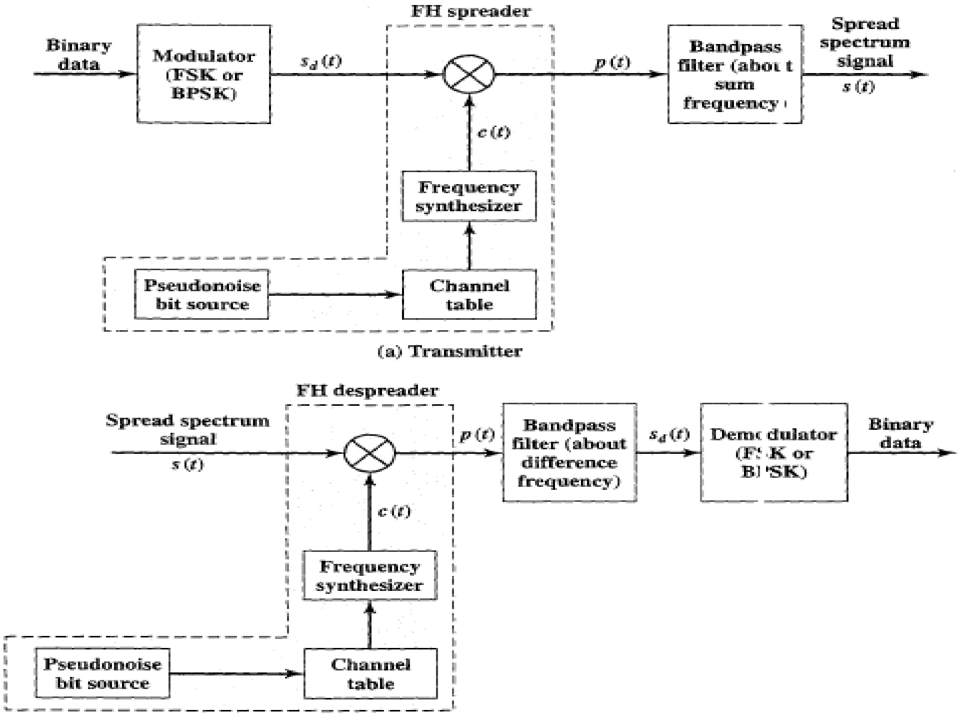


(a) Channel assignment

(b) Channel use

Following figure shows a typical block diagram for a hopping system.

- For transmission, binary data are fed into a modulator scheme using some digital-to-analog encoding scheme such as FSK or BPSK.
- PN used to index frequencies table
- Result centered on some base frequency
- Each interval, k bits of PN select frequency
- This freq is modulated with FSK/PSK signal
- Produce signal centered on new carrier
- Frequencies sorted as permuted table
- On reception, the spread spectrum signal is demodulated using the same sequence of PN derived frequencies and then demodulate the output data.



(a) Transmitter

(b) Receiver

- FHSS using BFSK

  We can define the FSK input to the FHSS system as :

$s_d(t)$=Acos(2PI(f0+0.5(bi+1) ∆f)t) for iT<t<(i+1)T

where A=amplitude of signal

f0= base frequency

bi=values of ith bit of data

∆ f= frequency separation

T= bit duration

1/T= data rate

The frequency synthesizer generates a constant frequency tone whose frequency hops among a set of 2^k frequencies with the hopping pattern determined by k bits from the PN sequence.

- FHSS Using MFSK

  MFSK commonly used with FHSS

  MFSk uses M=2L different frequency to encode the digit input L bits at a time.

  The transmitted signal is of the form:-

  Si(t)=Acos2PIfi t, 1<= I <=M

  Where fi=fc +(2i-1-M)fd

  Fc denotes the carrier frequency

  Fd denotes the difference frequency

  M denotes the number of signal element

  L denotes the no. of bits per signal element.

  MFSK signal modulated with FHSS carrier Translated to new channel every Tc sec

  For data rate R bit duration T = 1/R sec and the duration of signal element duration Ts = LT

  If the Tc is greater than or equal to Ts, the spreading modulation is referred to as Slow FHSS . Otherwise it is known as Fast FHSS.

Example

- M = 4 frequencies encode 2 bits at a time
- MFSK bandwidth Wd = 2M fd
- Using FHSS with k = 2, 2k = 4 channels
- Each channel with bandwidth Wd
- Total bandwidth for FHSS: Ws = 2kWd
- Slow FHSS: Tc = 2 Ts = 4 Tb
- channel held for duration of two signal elements
- Fast FHSS: Ts = 2 Tc = 2 Tb
- signal element represented in two channels

Example – Slow FHSS

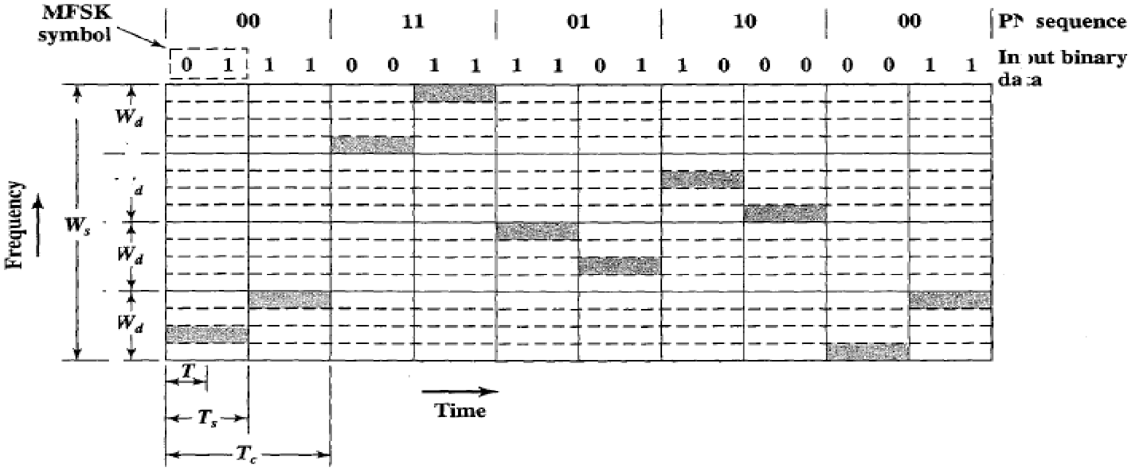


Figure Slow-Frequency-Hop Spread Spectrum Using MFSK ($M = 4, k = 2$)

Example – Fast FHSS

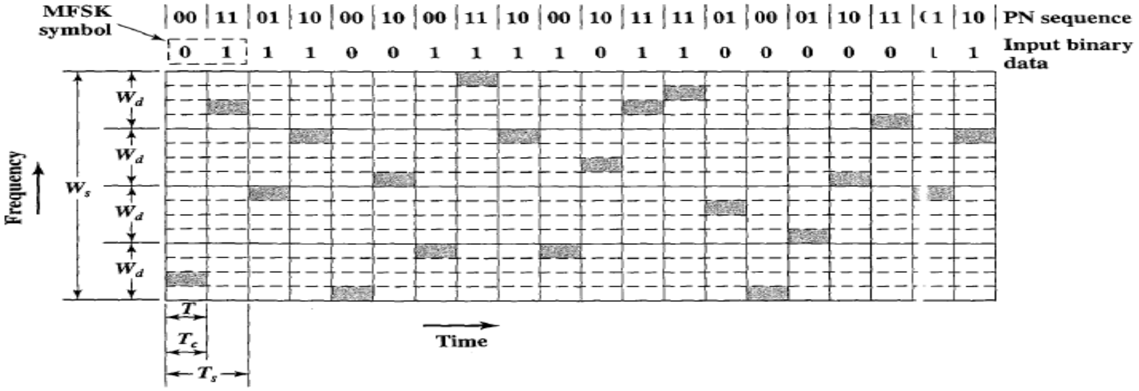


Figure Fast-Frequency-Hop Spread Spectrum Using MFSK ($M = 4, k = 2$)

FHSS Performance

- For MFSK
  Eb / Nj = (Eb Wd) / Sj
  Wd = bandwidth of MFSK signal
  Nj = jamming noise per hertz
  Sj = jamming power (Nj = Sj / Wd in this case)
  Eb = signal energy per bit
- FHSS Performance
- FHSS: jammer must jam all 2k frequencies
- Jamming power reduced to Sj / 2k
- Gain in S/N (processing gain)
- Gp = 2k = Ws / Wd
  Ws = FHSS signal bandwidth
- FHSS has strong resistance to jamming

Q 20) Discuss the application areas that are supported by Bluetooth. How the security is achieved in Bluetooth?

Ans: The concept of Bluetooth is to provide a universal short range wireless capability. The Bluetooth is intended to support an open ended list of applications, including data, audio, graphics and even video.

Bluetooth is designed to operate in an environment of many users. Up to eight devices can communicate in a small network called a piconet.

Ten of this piconet can coexist in the same coverage range of the Bluetooth radio. To provide security, each link is encoded and protected against eavesdropping and interference.

Bluetooth provides support for three general application areas using a short range wireless connectivity.

- Data and voice access points:-

  Bluetooth facilitates real time voice and data transmissions by providing effortless wireless connection of portable and stationary communication devices.
- Cable replacement:

  Bluetooth eliminates the need for numerous, often proprietary, cable attachments for connection of practically any kind of communication device.

  Connections are instant and are maintained even when devices are not within line of sight.

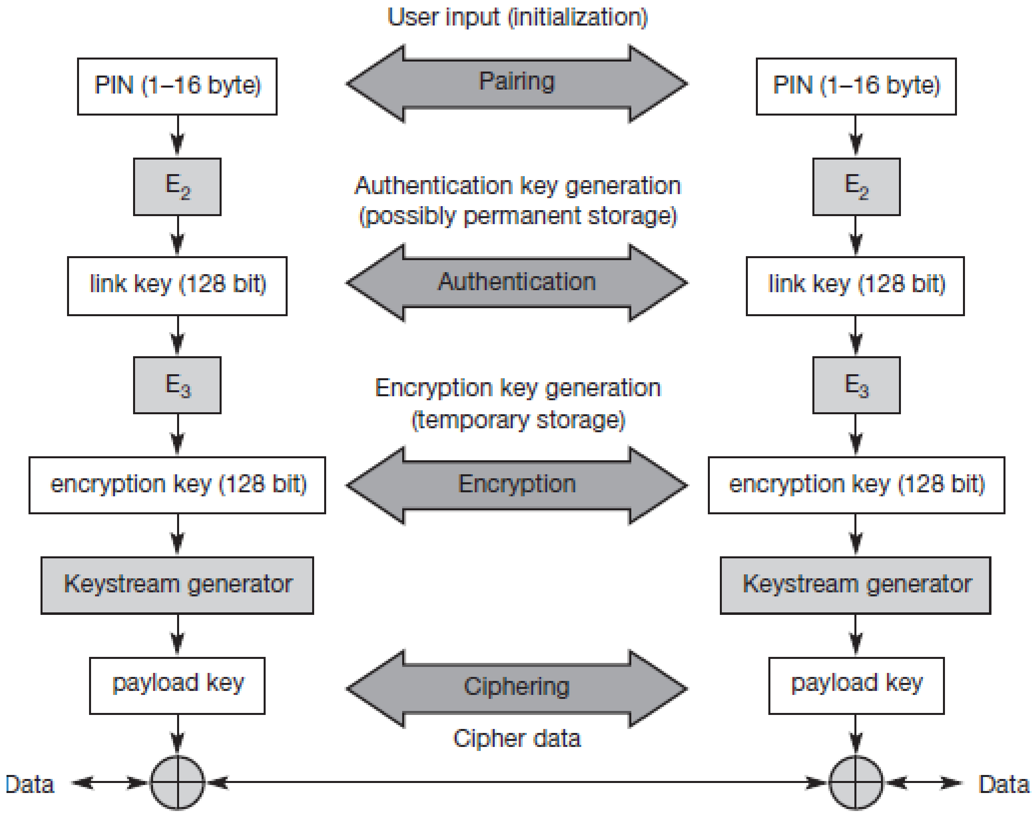
  The range of each radio is approximately 10m but can be extended to 100m with an optional amplifier.
- Ad hoc networking:

  A device equipped with a Bluetooth radio can establish instant connection to another Bluetooth radio as soon as it comes into range.

Security in Bluetooth:

- A radio interface is by nature easy to access. Bluetooth devices can transmit private data, e.g., schedules between a PDA and a mobile phone.
- A user clearly does not want another person to eavesdrop the data transfer. Just imagine a scenario where two Bluetooth enabled PDAs in suitcases ‘meet’ on the conveyor belt of an airport exchanging personal information.
- Bluetooth offers mechanisms for authentication and encryption on the MAC layer, which must be implemented in the same way within each device.
- The main security features offered by Bluetooth include a challengeresponse routine for authentication, a stream cipher for encryption, and a session key generation.

- Each connection may require a one-way, two-way, or no authentication using the challenge-response routine.
- All these schemes have to be implemented in silicon, and higher layers should offer stronger encryption if needed.
- The security features included in Bluetooth only help to set up a local domain of trust between devices.
- The security algorithms use the public identity of a device, a secret private user key, and an internally generated random key as input parameters.
- For each transaction, a new random number is generated on the Bluetooth chip. Key management is left to higher layer software.
- The first step, called **pairing**, is necessary if two Bluetooth devices have never met before. To set up trust between the two devices a user can enter a secret PIN into both devices. This PIN can have a length of up to 16 byte.
- Unfortunately, most devices limit the length to four digits or, even worse, program the devices with the fixed PIN '0000' rendering the whole security concept of Bluetooth questionable at least.
- Based on the PIN, the device address, and random numbers, several keys can be computed which can be used as link key for **authentication**.
- Link keys are typically stored in a persistent storage. The authentication is a challenge-response process based on the link key, a random number generated by a verifier (the device that requests authentication), and the device address of the claimant (the device that is authenticated).
- Based on the link key, values generated during the authentication, and again a random number an encryption key is generated during the **encryption** stage of the security architecture.
- This key has a maximum size of 128 bits and can be individually generated for each transmission.
- Based on the encryption Key, the device address and the current clock a payload key is generated for ciphering user data. The payload key is a stream of pseudo-random bits.
- The **ciphering** process is a simple XOR of the user data and the payload key.
- Compared to WEP in 802.11, Bluetooth offers a lot more security.
- However, Bluetooth, too, has some weaknesses when it comes to real implementations.
- The PINs are quite often fixed. Some of the keys are permanently stored on the devices and the quality of the random number generators has not been specified.
- If Bluetooth devices are switched on they can be detected unless they operate in the non-discoverable mode (no answers to inquiry requests). Either a user can use all services as intended by the Bluetooth system, or the devices are hidden to protect privacy. Either roaming profiles can be established, or devices are hidden and, thus many services will not work. If a lot of people carry.
- Bluetooth devices (mobile phones, PDAs etc.) this could give, e.g., department stores, a lot of information regarding consumer behavior.


User input (initialization)
PIN (1–16 byte)
Pairing
PIN (1–16 byte)
E2
Authentication key generation
(possibly permanent storage)
E2
link key (128 bit)
Authentication
link key (128 bit)
E3
Encryption key generation
(temporary storage)
E3
encryption key (128 bit)
Encryption
encryption key (128 bit)
Keystream generator
Keystream generator
payload key
Ciphering
payload key
Cipher data
Data
Data

Q 21) In Bluetooth technology what is a piconet and scatternet? What is active state v/s parked state?

Ans:

- A piconet is a collection of Bluetooth devices which are synchronized to the same hopping sequence.
- Figure 21.a shows a collection of devices with different roles. One device in the piconet can act as master (M), all other devices connected to the master must act as slaves (S).
- The master determines the hopping pattern in the piconet and the slaves have to synchronize to this pattern.
- Each piconet has a unique hopping pattern. If a device wants to participate it has to synchronize to this.

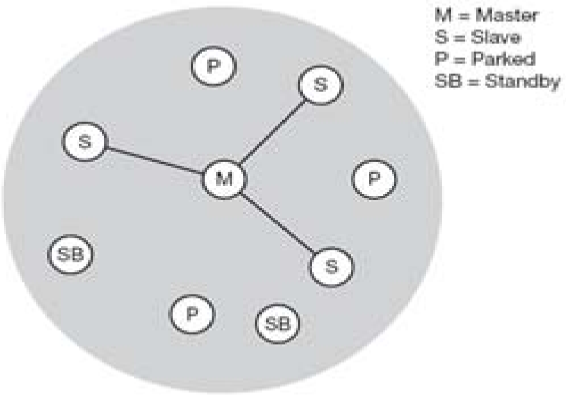


Fig. 21.a Simple Bluetooth piconet

- Two additional types of devices are shown: parked devices (P) can not actively participate in the piconet (i.e., they do not have a connection), but are known and can be reactivated within some milliseconds.
- Devices in stand-by (SB) do not participate in the piconet.
- Each piconet has exactly one master and up to seven simultaneous slaves.
- More than 200 devices can be parked. The reason for the upper limit of eight active devices, is the 3-bit address used in Bluetooth.
- If a parked device wants to communicate and there are already seven active slaves, one slave has to switch to park mode to allow the parked device to switch to active mode.
- Figure 21.b gives an overview of the formation of a piconet. As all active devices have to use the same hopping sequence they must be synchronized.
- The first step involves a master sending its clock and device ID. All Bluetooth devices have the same networking capabilities, i.e., they can be master or slave.

- There is no distinction between terminals and base stations, any two or more devices can form a piconet.

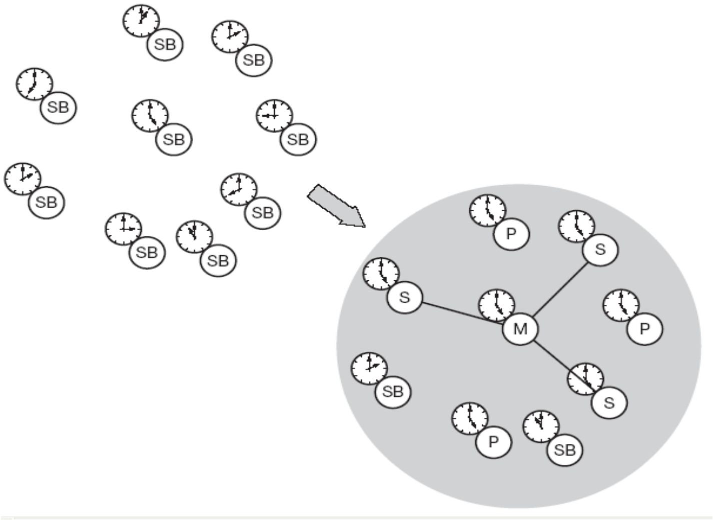


Fig. 21.b Forming a Bluetooth piconet

- The unit establishing the piconet automatically becomes the master, all other devices will be slaves.
- The hopping pattern is determined by the device ID, a 48-bit worldwide unique identifier.
- The phase in the hopping pattern is determined by the master's clock. After adjusting the internal clock according to the master a device may participate in the piconet.
- All active devices are assigned a 3-bit active member address (AMA). All parked devices use an 8-bit parked member address (PMA).
- Devices in stand-by do not need an address.
- All users within one piconet have the same hopping sequence and share the same 1 MHz channel.
- As more users join the piconet, the throughput per user drops quickly (a single piconet offers less than 1 Mbit/s gross data rate). (Only having one piconet available within the 80 MHz in total is not very efficient.)
- This led to the idea of forming groups of piconets called scatternet (see Figure 21.c).
- Only those units that really must exchange data share the same piconet, so that many piconets with overlapping coverage can exist simultaneously.
- In the example, the scatternet consists of two piconets, in which one device participates in two different piconets.
- Both piconets use a different hopping sequence, always determined by the master of the piconet.
- Bluetooth applies FH-CDMA for separation of piconets. In an average sense, all piconets can share the total of 80 MHz bandwidth available.

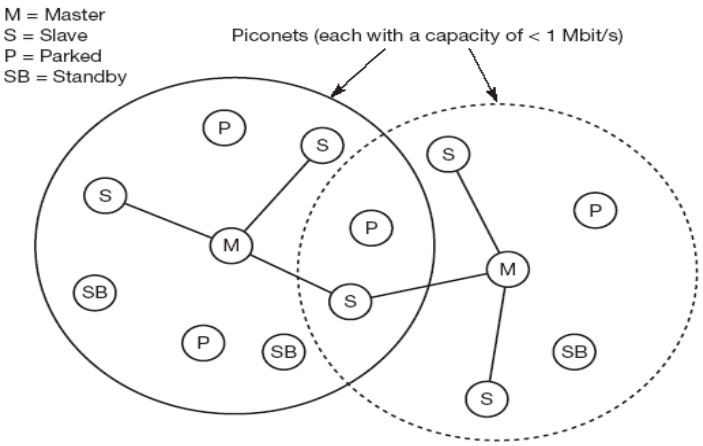


Fig. 21.c Bluetooth scatternet

- Adding more piconets leads to a graceful performance degradation of a single piconet because more and more collisions may occur.
- A collision occurs if two or more piconets use the same carrier frequency at the same time. This will probably happen as the hopping sequences are not coordinated.
- If a device wants to participate in more than one piconet, it has to synchronize to the hopping sequence of the piconet it wants to take part in.
- If a device acts as slave in one piconet, it simply starts to synchronize with the hopping sequence of the piconet it wants to join.
- After synchronization, it acts as a slave in this piconet and no longer participates in its former piconet.
- To enable synchronization, a slave has to know the identity of the master that determines the hopping sequence of a piconet.
- Before leaving one piconet, a slave informs the current master that it will be unavailable for a certain amount of time.
- The remaining devices in the piconet continue to communicate as usual. A master can also leave its piconet and act as a slave in another piconet.
- It is clearly not possible for a master of one piconet to act as the master of another piconet as this would lead to identical behavior (both would have the same hopping sequence, which is determined by the master per definition).
- As soon as a master leaves a piconet, all traffic within this piconet is suspended until the master returns.
- Communication between different piconets takes place by devices jumping back and forth between theses nets.
- If this is done periodically, for instance, isochronous data streams can be forwarded from one piconet to another. However, scatternets are not yet supported by all devices.

Q 22) What are the advantages and disadvantages of wireless LAN over wired LAN? Explain why CSMA/CD cannot be implemented in wireless LAN?

Ans: Advantages:

The following are the advantages of WLANs compared to their wired counterparts:

1. Flexibility:
   Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls, senders and receivers can be placed anywhere (also non-visible, e.g., within devices, in walls etc.). Sometimes wiring is difficult if firewalls separate buildings (real firewalls made out of, e.g., bricks, not routers set up as a firewall). Penetration of a firewall is only permitted at certain points to prevent fire from spreading too fast.
2. Planning:
   Only wireless ad-hoc networks allow for communication without previous planning, any wired network needs wiring plans. As long as devices follow the same standard, they can communicate. For wired networks, additional cabling with the right plugs and probably interworking units (such as switches) have to be provided.

3. Design:
   Wireless networks allow for the design of small, independent devices which can for example be put into a pocket. Cables not only restrict users but also designers of small PDAs, notepads etc. Wireless senders and receivers can be hidden in historic buildings, i.e., current networking technology can be introduced without being visible.

4. Robustness:
   Wireless networks can survive disasters, e.g., earthquakes or users pulling a plug. If the wireless devices survive, people can still communicate. Networks requiring a wired infrastructure will usually break down completely.

5. Cost:
   After providing wireless access to the infrastructure via an access point for the first user, adding additional users to a wireless network will not increase the cost. This is, important for e.g., lecture halls, hotel lobbies or gate areas in airports where the numbers using the network may vary significantly. Using a fixed network, each seat in a lecture hall should have a plug for the network although many of them might not be used permanently. Constant plugging and unplugging will sooner or later destroy the plugs. Wireless connections do not wear out.

Disadvantages:

1. Quality of service:

   WLANs typically offer lower quality than their wired counterparts. The main reasons for this are the lower bandwidth due to limitations in radio transmission (e.g., only 1–10 Mbit/s user data rate instead of 100–1,000 Mbit/s), higher error rates due to interference (e.g., 10–4 instead of 10–12 for fiber optics), and higher delay/delay variation due to extensive error correction and detection mechanisms.
2. Restrictions:

   All wireless products have to comply with national regulations. Several government and non-government institutions worldwide regulate the operation and restrict frequencies to minimize interference. Consequently, it takes a very long time to establish global solutions like, e.g., IMT-2000, which comprises many individual standards. WLANs are limited to low-power senders and certain license-free frequency bands, which are not the same worldwide.
3. Safety and security:

   Using radio waves for data transmission might interfere with other high-tech equipment in, e.g., hospitals. Senders and receivers are operated by laymen and, radiation has to be low. All standards must offer (automatic) encryption, privacy mechanisms, support for anonymity etc.
4. Easy to use:

   In contrast to huge and complex wireless WANs, wireless LANs are made for simple use. They should not require complex management, but rather work on a plug-and-play basis.
5. Global operation:

   WLAN products should sell in all countries so, national and international frequency regulations have to be considered. In contrast to the infrastructure of wireless WANs, LAN equipment may be carried from one country into another – the operation should still be legal in this case.

CSMA/CD cannot be implemented in wireless LAN:

- CSMA/CD is the MAC method used in a wired LAN (Ethernet).
- Wired LAN stations can whereas wireless stations cannot detect collisions.
- In case of WLAN, while transmitting, the strength of its own transmissions would mask all other signals in the air.
- So, the protocol can't directly detect collisions like with Ethernet and only tries to avoid them.
- However, on a wire, the transceiver has the ability to listen while transmitting and so to detect collisions.

Q 23) How is spread spectrum technique useful in wireless communication? Explain FHSS and DSSS.

Ans:

Spread spectrum:

Spread spectrum was originally developed to improve the reliability and security of radio transmissions (primarily for military communications systems). Prior to World War II, several famous individuals were involved in early research on frequency hopping spread spectrum applications including Nikola Tesla and Hedy Lamarr. Before Wi-Fi and cellular networks became popular, the telecommunications industry began rolling out various other applications of spread spectrum starting in the 1980s

Spread spectrum technology has blossomed from a military technology into one of the fundamental building blocks in current and next-generation wireless systems. From cellular to cordless to wireless LAN (WLAN) systems, spectrum is a vital component in the system design process.

Since spread-spectrum is such an integral ingredient, it's vital for designers to have an understanding of how this technology. In this tutorial, we'll take on that task, addressing the basic operating characteristics of a spread-spectrum system. We'll also examine the key differentiators between frequency-hop (FHSS) and direct-sequence spread spectrum (DSSS) implementations.

Spread spectrum approach to wireless communications is employed today in Wi-Fi and some cellular networks to obtain the following benefits:

- enhanced reliability - mitigates the impact of wireless interference on a communication channel
- increased bandwidth - exploits additional wireless spectrum to better utilize and share bandwidth among multiple channels
- improved security - limits the ability of attackers to intercept transmissions

The main idea behind spread spectrum is to separate a wireless communication into a set of related transmissions, send the messages over a wide range of radio frequencies, then collect and re-combine signals on the receiving side.

Several different techniques exist for implementing spread spectrum on wireless networks. Wi-Fi protocols utilize both *frequency hopping* and *direct sequence* spread spectrum.

FHSS:

FHSS is one of two types of spread spectrum radio, the other being direct-sequence spread spectrum. FHSS is a transmission technology used in LAWN transmissions where the data signal is modulated with a narrowband carrier signal that "hops" in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies. The signal energy is spread in time domain rather than chopping each bit into small pieces in the frequency domain. This technique reduces interference because a signal from a narrowband system will only affect the spread spectrum signal if both are transmitting at the same frequency at the same time. If synchronized properly, a single logical channel is maintained.

The transmission frequencies are determined by a spreading, or hopping, code. The receiver must be set to the same hopping code and must listen to the incoming signal at the right time and correct frequency in order to properly receive the signal. Current FCC regulations require manufacturers to use 75 or more frequencies per transmission channel with a maximum dwell time (the time spent at a particular frequency during any single hop) of 400 ms

DSSS:

DSSS is one of two types of spread spectrum radio, the other being frequency-hopping spread spectrum. DSSS is a transmission technology used in LAWN transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission.

Q 25) Explain in brief the operation the cellular systems

Ans: The operation of a cellular mobile system can be described as five major functionalities and four additional utilities. All the functions together make a complete mobile cellular system.

Mobile unit initialization

a. When mobile unit is turned on, it scans and selects the strongest setup control channel used for system.
b. Cells with different frequency bands repetitively broadcast on different setup channels.
c. The receiver selects the strongest setup channel and monitors that channel.
d. With this the mobile station has automatically selected the BS antenna of the cell within which it will operate.
e. Then handshake takes place b/w the mobile unit and MTSO controlling this cell through the BS in this cell.
f. Handshake is used to identify the user and register its location.
g. As long as the mobile station is on, scanning is repeated periodically to account for the motion of the unit.
h. If the unit enters a new cell, then a new BS is selected.

Mobile-originated call

a. A mobile unit originates a call by sending the number (Mobile Identification Number, MIN) of the called unit on the preselected setup channel.
b. The receiver of mobile unit checks if the forward channel (from BS) is idle.
c. If idle the mobile may transmit over the reverse channel(To base station)
d. BS sends request to the MTSO.

Paging

a. MTSO attempts to complete connection
b. MTSO sends a paging message to certain BSs depending on called mobile number.
c. BS sends paging signal on its own assigned setup channel.

Call accepted

a. Called mobile unit recognizes its number on the setup channel being monitored and responds to that BS, which sends the response to the MTSO.
b. MTSO sets up a circuit between calling and called BSs.
c. MTSO selects available traffic channel within each BS's cell and notifies each BS, which in turn notifies its mobile unit (a data message called alert is transmitted over FVC to instruct the mobile to ring).
d. The two mobile units tune to their respective channels.

Ongoing call

a. While connection is maintained, two mobile stations exchange voice or data, through BSs and MTSO.

Handoff

a. If a mobile unit moves from range of one cell to another the traffic channel has to change.
b. System makes this change without either interrupting the call or alerting the user.

Call blocking: If all traffic channels are busy even after multiple attempts a busy tone is returned.
Call termination: When one of the users hangs up, MTSO is informed and the traffic channels are released
Call drop: during a connection if because of interference or weak signal spots, the BS can't maintain the minimum required signal strength for a certain period of time the traffic channel is dropped and MTSO is informed.
Calls to/from fixed and remote mobile subscriber**:** MTSO connects to the public switched telephone network. Thus it can setup calls b/w mobile user in its area and fixed subscriber via telephone network, remote MTSO.

Q 26) Suppose a transmitter produces 50 W of power-

a. **Express transmit power in units of dBm and dBW**
b. **If the transmitter power in applied to unity gain antenna with 900MHz carrier frequency what is the received power in dBm at a free space distance of 10 m.**

Ans:

a.) $\text{Power}_{(\text{dBW})} = 10 \log (\text{Power}_{\text{W}})$

$= 10 \log (50)$

$= 17$ dBWPower

$\text{Power}_{(\text{dBm})} = 10 \log (\text{Power}_{\text{mW}})$

$= 10 \log (50{,}000)$

$= 47$ dBm

b.) $L_{\text{dB= 20 log (f) 20 log (d) - 147.56 dB}}$

$= 20 \log (900\times10^{6}) + 20 \log (10) - 147.56$

$= 120 + 59.08 + 20 - 147.56$

$= 51.52$

Therefore, received power in dBm = 47 – 51.52

= –4.52 dBm

Q 27) What is antenna? Explain the different types of antennas and the radiation pattern of each of them.

Ans:

Antenna:

1. An antenna can be defined as an electrical conductor or system of conductors used either for radiating electromagnetic energy into the space or for collecting electromagnetic energy from the space.

2. For the transmission of the signal, radio-frequency electrical energy from the transmitter is converted into electromagnetic energy by the antenna and radiated into the surrounding environment.

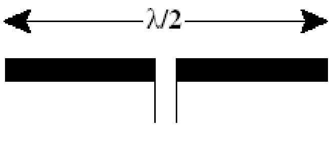
3. For reception of a signal, electromagnetic energy impinging on the antenna is converted into radio-frequency electrical energy and fed into the receiver.

Antenna Types:

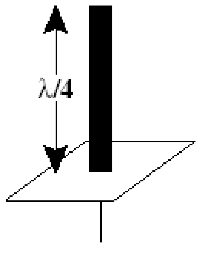
1. Dipoles:

Two of the simplest and most basic antennas are the half-wave dipole or hertz, antenna and the quarter wave vertical, or Marconi, antenna. The half-wave dipole consists of two straight collinear conductors of equal length, separated by a small feeding gap. The length of the antenna is one-half the wavelength of the signal that can be transmitted most efficiently. A vertical quarter-wave antenna is the type commonly used for automobile radios and portable radios.

A half-wave dipole has a uniform or omnidirectional radiation pattern in one dimension and a figure eight pattern in the other two dimensions. More complex antenna configurations can be used to produce a directional beam. A typical directional radiation pattern is shown in the figure below. In this case the strength of the antenna is in the x direction.



(a) Half-wave dipole



(b) Quarter-wave antenna

Fig 1.1

2. Parabolic Reflective Antenna :

An important type of antenna is the parabolic reflective antenna, which is used in terrestrial microwave and satellite applications. A parabola is the locus of all points equidistant from a fixed line and a fixed point not on the line. The fixed point is called the focus and the fixed line is called the directrix.If a parabola is revolved about the axis, the surface generated is called a paraboloid.A cross section through the parabolic parallel to its axis forms a parabola and a cross section perpendicular to the axis forms a circle. Such surfaces are used in headlights, optical and radio telescope and microwave antennas because of the following property. If a source of electro-magnetic energy is placed at the focus of the paraboloid and if the paraboloid is a reflecting surface, then the wave will bounce back in lines parallel to the axis of the paraboloid. The following figure shows this effect in cross section:

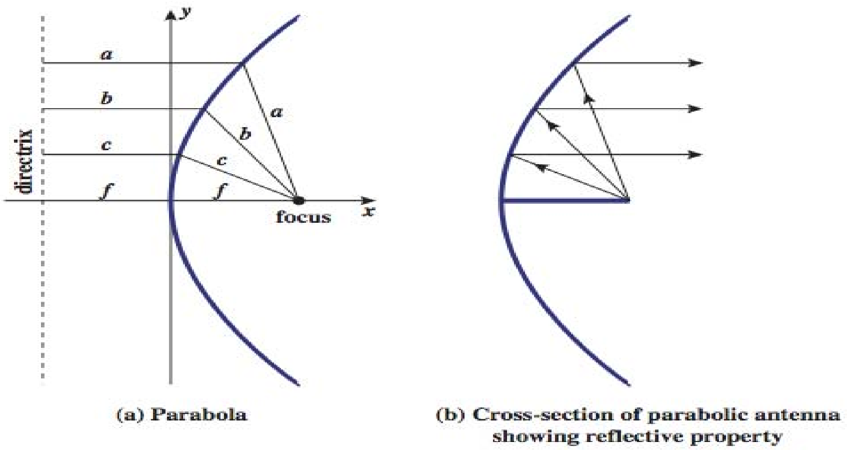

y
a
b
c
f
directrix
a
b
c
f
focus
x
(a) Parabola
(b) Cross-section of parabolic antenna showing reflective property

Fig 1.2

The following figure shows a typical radiation pattern for the parabolic reflective antenna. The larger the diameter of the antenna, the more tightly directional is the beam.

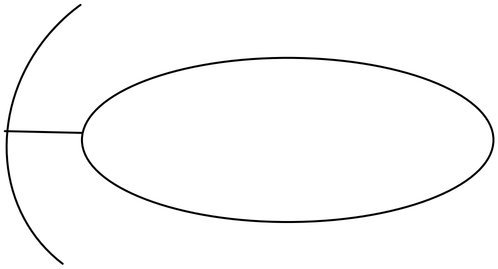


Fig 1.3 Cross section of parabolic antenna showing radiation pattern

Q.28) Compare the different generations of cellular systems.

Ans:

Sr.	First Generation	Second Generation	Third Generation
1	First generation systems are almost purely analog.	Second generation system are digital.	Third generation system are digital. This has the highest bandwidth and multimedia support at amazing speed.
2	Protocol for accessing the channel is FDMA.	Protocol for accessing the channel CDMA, TDMA.	Protocol for accessing the channel CDMA, TDMA.
3	Modulation Technique used FM, FSK.	Modulation Technique used QPSK.	Modulation Technique used QPSK(forward), BPSK (reverse).
4	Handoff strategies used is Hard Handoff	Handoff strategies used is Soft Handoff.	Handoff strategies used is Soft Handoff.
5	Technology used is Advance Mobile Phone Service (AMPS).	Technology used is IS-QS GSM (Global System For Mobile Communication).	Second Generation has multiple standards. This is the biggest disadvantage. Second Generation networks consist of CDMA, GSM and other standards. This causes problem during roaming. On the other hand, 3G has integrated standards.
6	No error detection and correction technique is used.	Parity check, CRC can be used for error detection and Block codes and Convolution codes can be used for error detection and correction.	Comparing the data rate, Third Generation has higher data rate compared to Second Generation.

7	User traffic is clear. No encryption required.	It is encrypted.	Second Generation is voice centric. Second Generation was made with the main goal of voice communication. Third Generation is multimedia centric, which means it has a primary job to carry out data.
8	Each cell supports a number of channels. At any given time a channel is allocated to only one user.	Each cell can support multiple channels. But each channel is dynamically shared by a no. of users using TDMA or CDMA.	Third Generation network offers wider bandwidth. This enables Third Generation to carry more data at more speed.
9	These systems are designed to support voice channels using FM. Digital traffic is supported only by use of modem that converts digital data into analog form.	These systems provide digital traffic channels voice traffic is first encoded in digital form before transmitting.	Third Generation has a common spectrum worldwide. This results in seamless global connectivity.
10	In these systems user traffic is send directly without any security.	As all users' traffic control traffic is digitized, it is simpler to encrypt all of the traffic to prevent eavesdropping.	Third Generation has improved security and performance.

Q.29) Explain the different transmission techniques used in the infrared LANs.

Ans: Different transmission techniques used in the infrared LANs are as follows:

1. Direct Beam Infrared

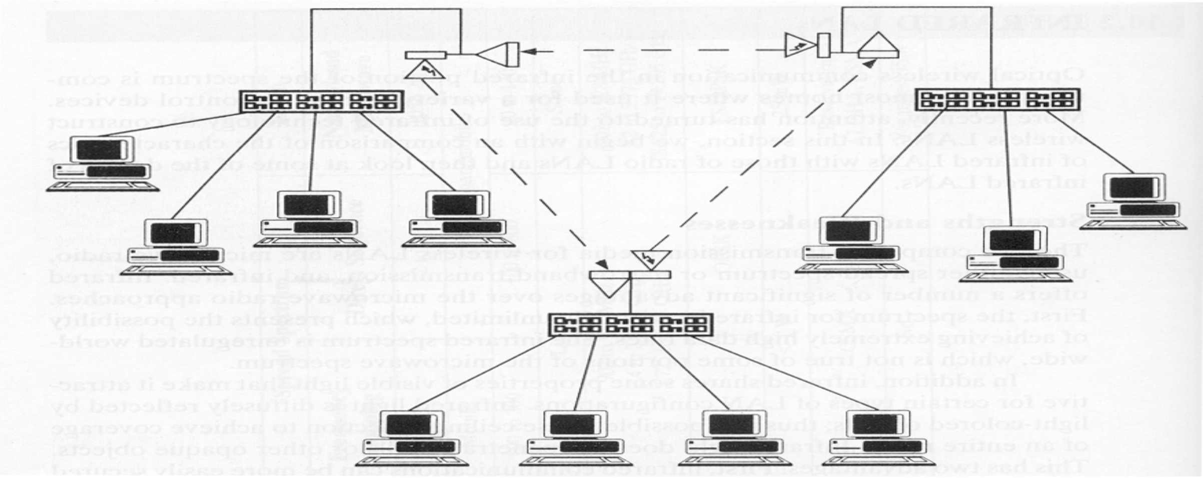
    a) Used to create point-to-point links.

    b) Depending on the emitted power and on the degree of focusing.

    c) Used for cross-building inter-connect between bridges or routers located in buildings within a line of sight of each other.

    d) For example, setting up a token ring LAN.

Token ring LAN using point-to-point infrared Links



2. Omni Directional

    a) Omni directional configuration involves a single base station that is within line of sight of all other stations on the LAN.

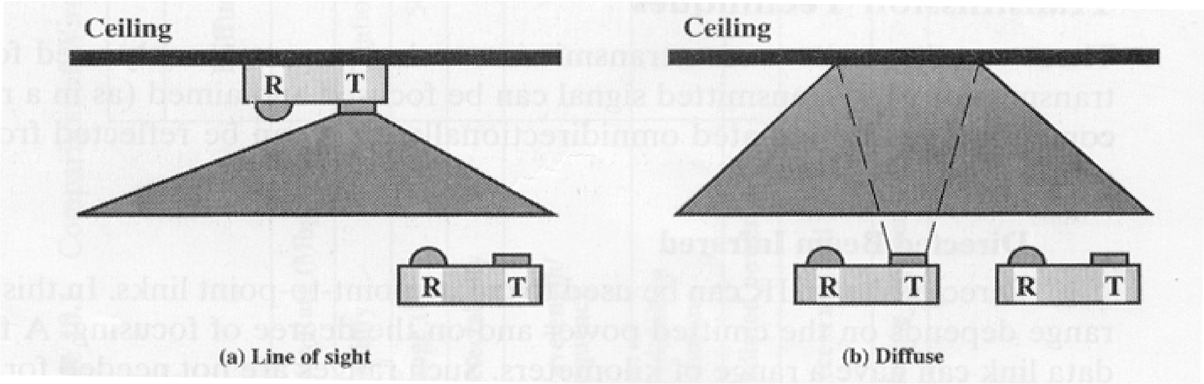
    b) The base station acts as a multiport repeater similar to the type for 10BASE-T and 100BASE-T.

3. Diffused

    a) All of IR transmitters are focused and aimed at a point a diffusely reflecting ceiling

b) IR radiation striking the ceiling is reradiated Omni directionally and picked up by all of the receivers in the area

Configurations for Diffused Infrared LANs



(a) Line of sight (b) Diffuse

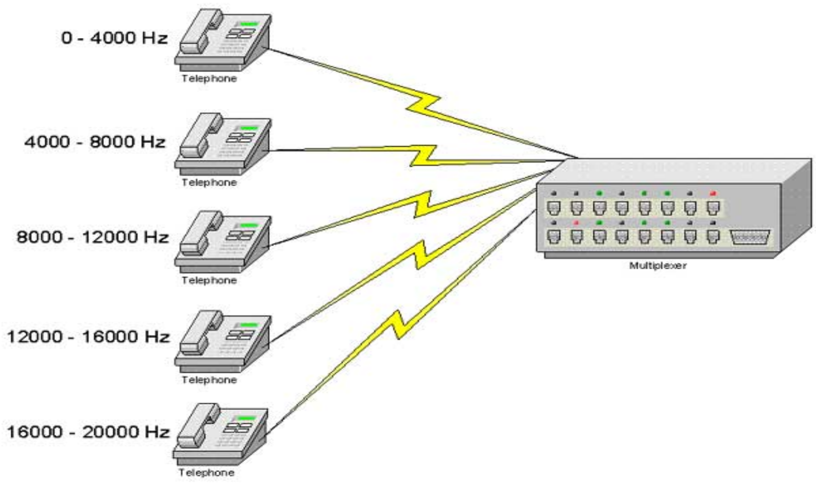
Q.30 Explain the modulation techniques FDM and CDMA?

Ans:

<u>Frequency Division Modulation (FDM):</u>

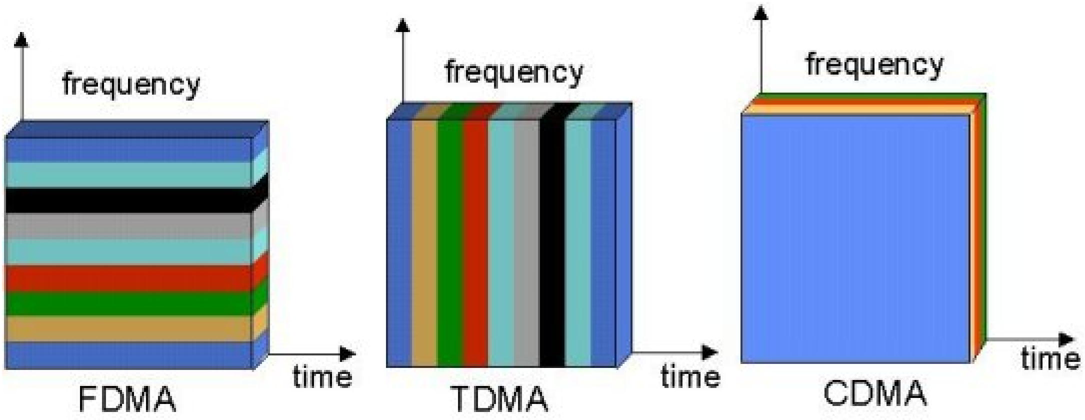
- *Frequency division multiplexing* (FDM) means that the total bandwidth available to the system is divided into a series of non-overlapping frequency sub-bands that are then assigned to each communicating source and user pair

- Frequency-division multiplexing (FDM) is inherently an analog technology
- One of FDM's most common applications is cable television. Only one cable reaches a customer's home but the service provider can send multiple television channels or signals simultaneously over that cable to all subscribers. Receivers must tune to the appropriate frequency (channel) to access the desired signal.[
- FDM was developed to work with early telephone networks. It worked by dividing the frequencies to support multiple users. For instance, with a standard sound spectrum (20 Hz - 20,000 Hz) the frequencies would be equally divided to support 5 or so users per physical line. Note that in this case, users are given some of the frequency all the time. FDM is still used with cable TV, some older analog cellular systems, and most commonly YOUR FM RADIO! See the figure below:



<u>Code division multiple access (CDMA):</u>

- In Code Division Multiple Access (CDMA), every communicator will be allocated the entire spectrum all of the time. CDMA uses codes to identify connections.



CODING

- CDMA uses unique spreading codes to spread the baseband data before transmission. The signal is transmitted in a channel, which is below noise level.
- The receiver then uses a correlator to despread the wanted signal, which is passed through a narrow bandpass filter. Unwanted signals will not be despread and will not pass through the filter. Codes take the form of a carefully designed one/zero sequence produced at a much higher rate than that of the baseband data. The rate of a spreading code is referred to as chip rate rather than bit rate.

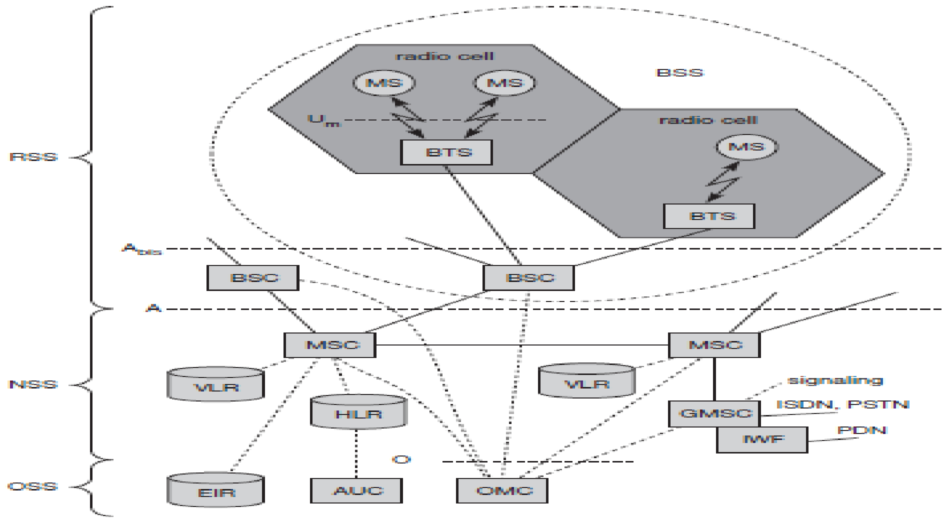
Advantages of CDMA:

- Frequency diversity:
  Because the transmission is spread out over a larger bandwidth, frequency- dependent transmission impairments, such as noise burst and selective fading, have less effect on the signal.
- Multipath resistance:
  One of the main advantages of CDMA systems is the capability of using signals that arrive in the receivers with different time delays. This phenomenon is called multipath.
- Graceful degradation:
  With CDMA , as more user access the system simultaneously, the noise level and hence the error rate increases; only gradually does the system degrade to the point of an unacceptable error rate.

Q 31) Discuss the GSM architecture. What are the techniques used to provide data packets in GSM?

Ans:

GSM Architecture:



A GSM network consists of the following components:

- Mobile station. The GSM mobile station (or mobile phone) communicates with other parts of the system through the base-station system.
- GSM Base station system (BSS).
- Base transceiver station (BTS). The base transceiver station (BTS) handles the radio interface to the mobile station. The base transceiver station is the radio equipment (transceivers and antennas)
- Base station controller (BSC). The BSC provides the control functions and physical links between the MSC and BTS. It provides functions such as handover, cell configuration data and control of RF power levels in base transceiver stations. A number of BSCs are served by a MSC.
- GSM Switching System
- Mobile services switching center (MSC). The MSC performs the telephony switching functions of the system. It also performs such functions as toll ticketing, network interfacing, common channel signalling, and others.
- Home location register (HLR). The HLR database is used for storage and management of subscriptions. The home location register stores permanent data about subscribers, including a subscriber's service profile, location information, and activity status.
- Visitor location register (VLR). The VLR database contains temporary information about subscribers that is needed by the mobile services switching center (MSC) in order to service visiting subscribers. When a mobile station roams into a new mobile services

switching center (MSC) area, the visitor location register (VLR) connected to that MSC will request data about the mobile station from the HLR, reducing the need for interrogation of the home location register (HLR).

- Authentication center (AUC). The AUC provides authentication and encryption parameters that verify the user's identity and ensure the confidentiality of each call. The authentication center (AUC) also protects network operators from fraud.
- Equipment identity register (EIR). The EIR database contains information on the identity of mobile equipment to prevent calls from stolen, unauthorized or defective mobile stations.
- Message center (MXE). The MXE is a node that provides integrated voice, fax, and data messaging.
- Mobile service node (MSN). The MSN is the node that handles the mobile intelligent network (IN) services.
- Gateway mobile services switching center (GMSC). A gateway mobile services switching center (GMSC) is a node used to interconnect two networks.
- GSM interworking unit (GIWU). The GIWU consists of both hardware and software that provides an interface to various networks for data communications. Through the GSM interworking unit (GIWU), users can alternate between speech and data during the same call.
- Operation and support system (OSS). The OSS is the functional entity from which the network operator monitors and controls the system. The purpose of operation and support system is to offer support for centralized, regional, and local operational and maintenance activities that are required for a GSM network.

The techniques used to provide data packets in GSM are:

1. Short Message Service(SMS):
    - It is a communication protocol allowing the interchange of short text messages between mobile telephone devices.
    - Typically a text message originating at a handset is sent to a Short Message Service Centre(SMSC).
    - The SMSC then attempts to send the message to its recipient.
    - If the recipient is not reachable, the SMSC queues the message for later retry.
    - This mechanism is characterized as a store-and-forward delivery system and SMS message transmission is characterized as best effort because there are no guarantees that the message will actually be delivered to the recipient.
2. General Packet Radio Service(GPRS):
    - The General Packet Radio Service (GPRS), like the name suggests is a mobile communication standard based on packet switched radio transmission.
    - Traffic channels are allotted only when needed and is released immediately after the transmission of packet is over. GPRS also allow for a user to be allotted multiple channels, leading to higher data rates.

Q 34) List the transmission impairment effecting the wireless transmission. Explain free space loss? Determine the free space loss at 4 GHz for the shortest path to a geo synchronous satellite?

Ans: Analog signal consist of varying a voltage with time to represent an information steam. If the transmission media were perfectly, the receiver could receive exactly the same signal that the transmitter sent. But communication lines are usually not perfect, so the receive signal is not the same as the transmitted signal. For digital data this difference can lead to errors. Transmission lines suffers from three major problems

1. Attenuation
2. Delay distortions
3. Noise

Attenuation:

It is the loss of energy as the signal propagates outward. The amount of energy depends on the frequency. If the attenuation is too much, the receiver may not be able to detect the signal at all, or the signal may fall below the noise level. For reliable communication, the attenuation and delay over the range of frequencies of transmission should be constant.

Distortion:

The second transmission impairment is delay distortion. Communication line have distributed inductance and capacitance which distort the amplitude of signals and also delay the signals at different frequencies by different amounts. It is caused by the fact that different Fourier components travel at different speed.

Noise:

Noise is a third impairment. It can be define as unwanted energy from sources other than the transmitter. Thermal noise is caused by the random motion of the electrons in a wire and is unavoidable.

Cross talk:

Similarly cross talk is a noise that is caused by the inductive coupling between two wires that are closed to each other. Sometime when talking on the telephone, you can hear another conversation in the background. That is cross talk

Free space path loss basics

The free space path loss, also known as FSPL is the loss in signal strength that occurs when an electromagnetic wave travels over a line of sight path in free space. In these circumstances there are no obstacles that might cause the signal to be reflected refracted, or that might cause additional attenuation.

The free space path loss calculations only look at the loss of the path itself and do not contain any factors relating to the transmitter power, antenna gains or the receiver sensitivity levels. These factors are normally address when calculating a link budget and these will also be used within radio and wireless survey tools and software.

To understand the reasons for the free space path loss, it is possible to imagine a signal spreading out from a transmitter. It will move away from the source spreading out in the form of a sphere. As it does so, the surface area of the sphere increases. As this will follow the law of the conservation of energy, as the surface area of the sphere increases, so the intensity of the signal must decrease.

As a result of this it is found that the signal decreases in a way that is inversely proportional to the square of the distance from the source of the radio signal.

$$\text{Signal} = \frac{1}{\text{distance}^2}$$

The equation for FSPL is

$$\begin{aligned} \mathrm{FSPL} &= \left(\frac{4\pi d}{\lambda}\right)^2 \\ &= \left(\frac{4\pi d f}{c}\right)^2 \end{aligned}$$

Decibel version of free space path loss equation

Most RF comparisons and measurements are performed in decibels. This gives an easy and consistent method to compare the signal levels present at various points. Accordingly it is very convenient to express the free space path loss formula, FSPL, in terms of decibels. It is easy to take the basic free space path loss equation and manipulate into a form that can be expressed in a logarithmic format.

FSPL (dB) = 20 $\log_{10}$ (d) + 20 $\log_{10}$ (f) + 32.44

Where:

d is the distance of the receiver from the transmitter (km)

f is the signal frequency (MHz)

Shortest path to a geo synchronous satellite is approximately 35000km .Frequency given is 4GHz i.e. 4000MHz approx.

FSPL(db)=20log 35000+20 log 4000+32.44

= 20*4.54+20*3.6+32.44

=90.8+72+32.44=195.24

Q 35) How is the security provided in the WAP using the wireless trans ort layer security?

Ans: WTLS can provide different levels of security (for privacy, data integrity, and authentication) and has been optimized for low bandwidth, high-delay bearer networks. WTLS takes into account the low processing power and very limited memory capacity of the mobile devices for cryptographic algorithms. WTLS supports datagram and connection-oriented transport layer protocols. New compared to, e.g. GSM, is the security relation between two peers and not only between the mobile device and the base station (see chapter 4). WTLS took over many features and mechanisms from TLS, but it has an optimized handshaking between the peers.

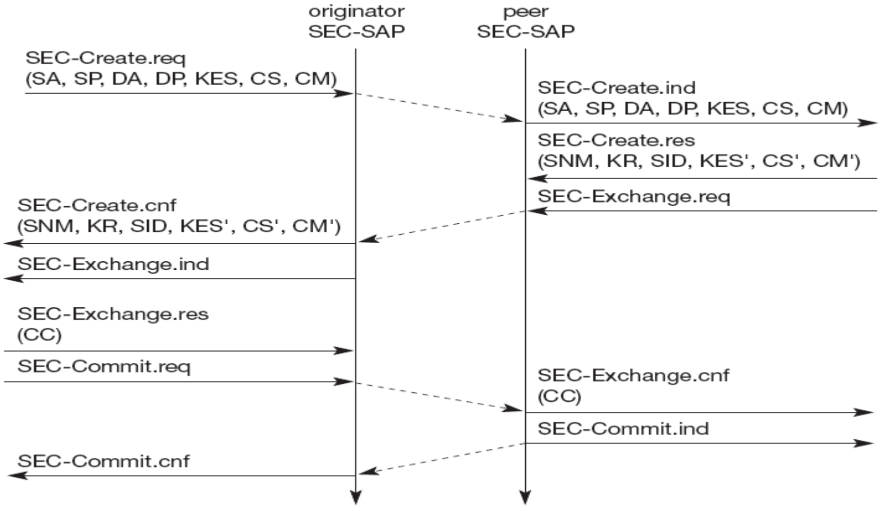
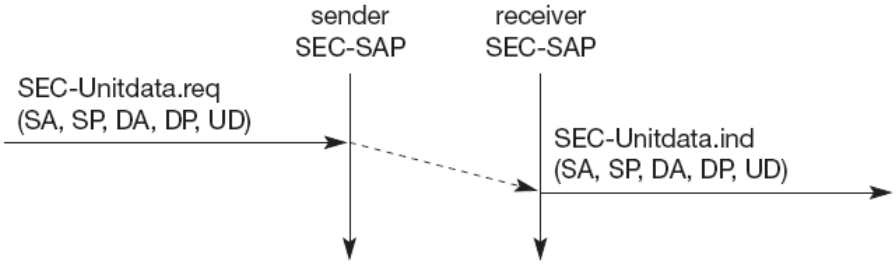


Figure: WTLS establishing a secure session.

Before data can be exchanged via WTLS, a secure session has to be established. This session establishment consists of several steps: Figure illustrates the sequence of service primitives needed for a so-called ‘full handshake’ (several optimizations are possible). The originator and the peer of the secure session can both interrupt session establishment any time, e.g., if the parameters proposed are not acceptable.

The first step is to initiate the session with the **SEC-Create** primitive. Parameters are **source address (SA), source port (SP)** of the originator, **destination address (DA), destination port (DP)** of the peer. The originator proposes **a key exchange suite (KES)** (e.g., RSA (Rivest, 1978), DH (Diffie, 1976), ECC (Certicom, 2002)), a **cipher suite (CS)** (e.g., DES, IDEA (Schneier, 1996), and **a compression method (CM)** (currently not further specified). The peer answers with parameters for the **sequence number mode (SNM)**, the **key refresh** cycle (**KR**) (i.e., how often keys are refreshed within this secure session), the **session identifier (SID)** (which is unique with each peer), and the selected **key exchange suite (KES’), cipher suite (CS’), compression method (CM’)**. The peer also issues a **SEC-Exchange primitive**. This indicates that the peer wishes to perform public-key authentication with the client, i.e., the peer requests a **client certificate (CC)** from the originator.



WTLS datagram transfer

After setting up a secure connection between two peers, user data can be exchanged. This is done using the simple **SEC-Unitdata** primitive as shown in Figure 10.13. SEC-Unitdata has exactly the same function as T-DUnitdata on the WDP layer, namely it transfers a datagram between a sender and a receiver. This data transfer is still unreliable, but is now secure. This shows that WTLS can be easily plugged into the protocol stack on top of WDP. The higher layers simply use SEC-Unitdata instead of T-DUnitdata. The parameters are the same here: **source address (SA), source port (SP), destination address (DA), destination port (DP),** and **user data (UD)**.

This section will not discuss the security-related features of WTLS or the pros and cons of different encryption algorithms. The reader is referred to the specification (WAP Forum, 2000c) and excellent cryptography literature e.g., (Schneier, 1996), (Kaufman, 1995). Although WTLS allows for different encryption mechanisms with different key lengths, it is quite clear that due to computing power on the handheld devices the encryption provided cannot be very strong. If applications require stronger security, it is up to an application or a user to apply stronger encryption on top of the whole protocol stack and use WTLS as a basic security level only. Many programs are available for this purpose. It is important to note that the security association in WTLS exists between the mobile WAP-enabled device and a WAP server or WAP gateway only. If an application accesses another server via the gateway, additional mechanisms are needed for end-to-end security. If for example a user accesses his or her bank account using WAP, the WTLS security association typically ends at the WAP gateway inside the network operator’s domain. The bank and user will want to apply additional security mechanisms in this scenario.

Q 36) Discuss the operation of mobile IP

Ans. Mobile IP was developed to enable computers to maintain Internet Connectivity while moving from one Internet attachment point to another. Although mobile IP can work with wired connections, in which a computer is unplugged from one physical attachment point and plugged into another, it is particularly suited to wireless connections.

Operation of Mobile IP:

A mobile node is assigned to a particular network, known as its home network. Its IP address on that network, known as its home address, is static. When the mobile mode moves its attachment point to another network is considered a foreign network for this host. Once the mobile node is reattached, it makes its presence known by registering with a network node, typically a router, on the foreign network known as foreign agent. The mobile node then communicates with a similar agent on the user's home network, known as home agent, giving the home agent the care-of-address of the mobile node (care-of-address identifies the foreign agent's location). Typically, one or more routers on a network will implement the roles of both home and foreign agents.

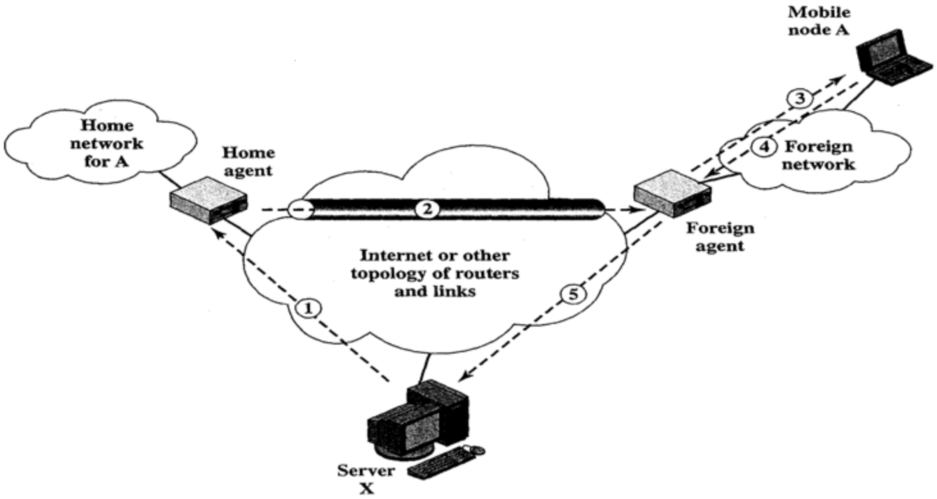


Fig: Mobile IP scenario

When IP datagrams are exchanged over a connection between the mobile node and another host, the following operations occur.

1. Server X transmits an IP datagram destined for mobile node A, with A's home address in the IP header. The IP datagram is routed to A's home network.
2. At the home network, the incoming IP datagram is intercepted by the home agent. The home agent encapsulates the entire datagram inside a new IP datagram that has A's care-of-address in the header, and retransmits the datagram. The use of an outer IP datagram

with a different destination IP address is known as Tunneling. This IP datagram is routed to the foreign agent.

3. The foreign agent strips off the outer IP header, encapsulates the original IP datagram in a network-level PDU, and delivers the original datagram to A across the foreign network.
4. When A sends IP traffic to X, it used X's IP address. In this example, this is a fixed address i.e. X is not a mobile node. Each IP datagram is sent by A to a router on the foreign network for routing to X. typically, this router is also the foreign agent.
5. The IP datagram from A to X travels directly across the Internet to X, using X's IP address.

To support the above operations, Mobile IP includes 3 basic capabilities.

- Discovery: A mobile node uses a discovery procedure to identify prospective home agents and foreign agents.
- Registration: A mobile node uses an authenticated registration procedure to inform its home agent of its care-of-address.
- Tunneling: This is used to forward IP datagrams from a home address to a care-of-address.

The diagram below indicates the underlying protocol support for Mobile IP capability. The registration protocol communicates between an application on the mobile node and an application in the home agent and hence uses a transport-level protocol. UDP is used as the transport protocol as it's a simple request-response transaction. Discovery makes use of existing ICMP(Internet Control Message Protocol) by adding the appropriate extensions to the ICMP header. ICMP is a connectionless protocol well suited for discovery operation. Finally, tunneling is performed at the IP level.

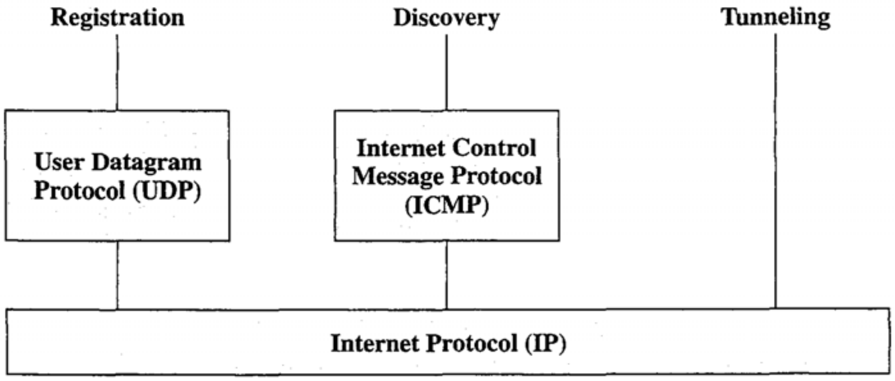

Registration
Discovery
Tunneling
User Datagram Protocol (UDP)
Internet Control Message Protocol (ICMP)
Internet Protocol (IP)

Fig: Protocol Support for Mobile IP

Discovery:

The agent discovery makes use of ICMP router advertisement messages, with one or more extensions specific to Mobile IP. The mobile node is responsible for an on-going discovery process. It must determine if it is attached to its home network, in which case the IP datagram may be received without forwarding; or if it attached to a foreign network. Because handoff from on network to another occurs at the physical layer, a transition from home network to foreign network can occur anytime, without any notification to the network later. Thus, discovery for a mobile node is a continuous process.

For the purpose of discovery, a router or other network node that can act as an agent periodically issues a router advertisement ICMP message. A mobile node listens for these agent advertisement messages. The mobile node must compare the network portion of the router's IP address with the network portion of its own home address. If these network portions do not match, then the mobile node is on foreign network.

Registration:

Once a mobile node has recognised that it is on foreign network and has acquired a care-of-address, it needs to alert a home agent on its home network and request that the home agent forward its IP traffic. The registration process involves the following four steps:

1. The mobile node requests the forwarding service by a registration request to the foreign agent that the mobile node wants to use.
2. The foreign agent relays this request to the mobile node's home agent.
3. The home agent either accepts or denies the request and sends a registration reply to the foreign agent.
4. The foreign agent relays the reply to the mobile agent.

Tunneling:

Once a mobile node is registered with a home agent, the home agent must be able to intercept IP datagrams sent to the mobile node's home address so that these datagrams can be forwarded via tunneling. The standard does not mandate a specific technique for this purpose but references ARP as a possible mechanism. The home agent needs to inform other nodes on the same network that IP datagrams with a destination address of the mobile node in question should be delivered to this agent. In effect, the home agent steals identity of the mobile node in order to capture packets destined for that node that are transmitted across the home network.

Q 37) Explain the application of wireless LAN.

Ans. There are four application areas for wireless LAN.

1. LAN Extension
2. Cross-building inter-connect
3. Nomadic access
4. Ad-hoc networks

LAN Extension:

Early wireless LAN products were marketed as substitutes for traditional wired LANs as wireless LAN saved the cost of installation of LAN cabling and eased the task of relocation and other modifications to network.

- The motivation for wireless LANs has overtaken by the following events:
    - ➢ As awareness of the need for LANs became greater, architects designed new buildings to include extensive pre-wiring for data applications.
    - ➢ With advances in data transmission technology, there is an increasing reliance on twisted pair cabling for LANs and in particular Category-3 and Category-5 unshielded twisted pair. Most older buildings have abundance of Category-3 wiring, and many newer buildings have been pre-wired by Category-5 cables. This is the reason that the use of wireless LAN to replace wired LANs has not happened to any great extent.
- Wireless LANs have replaced wired LAN in the following environments.
    - ➢ Buildings with large open areas, such as manufacturing plants, stock exchange trading floors, and warehouses; historical buildings with insufficient twisted pair and where drilling for new wires is prohibited; and small offices where installation and maintenance of wired LANs is not economical.
    - ➢ In cases like above, some organization also support wired LAN to support servers and some stationary workstation.
- Typically, a wireless LAN will be linked into a wired LAN on the same premises. Thus, this application area is referred to as LAN Extension.
- There are 2 configuration possible for wireless LANs – a.) Simple Wireless LAN configuration and b.) Multiple-Cell Wireless LAN.

Cross-Building Inter-connect:

- This is used to connect LANs in nearby buildings, be they wired or wireless LANs.
- A point-to-point wireless link is used between two buildings.
- The devices so connected are typically bridges and routers.

- This single point-to-point link is not a LAN, but it is usual to include this application under heading of wireless LAN.

Nomadic Access:

- This provides a wireless link between a LAN hub and a mobile data terminal equipped with an antenna, such as laptop computer or notepad computer.
- Example: to enable an employee returning from a trip to transfer data from a personal portable computer to a server in the office.
- This type is also useful in an extended environment such as campuses or a business operating out of a cluster of buildings. In both of these cases, the users may move around with their portable computers and may wish access to the servers on a wired LAN from various locations.

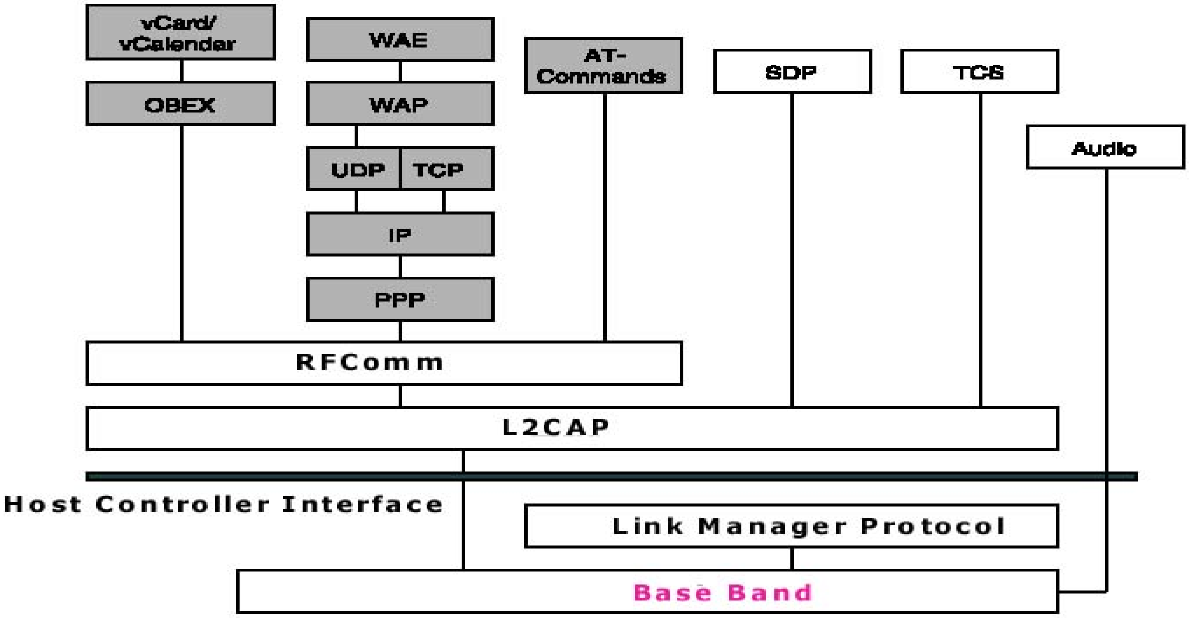
Ad-Hoc Networking:

- This is peer-to-peer network set up temporarily to meet some immediate need.
- Example: a group of employees, each with a laptop or palmtop computer, may convene in a conference room for a business or classroom meeting. The employees link their computers in a temporary network just for the duration of the meeting.

Q 38) Discuss the protocol architecture of Bluetooth.

Ans:

Bluetooth Protocol Architecture:



Controller stack

Asynchronous connection-oriented [Logical Transport] (ACL)

The normal type of radio link used for general data packets using a polling TDMA scheme to arbitrate access. It can carry several different packet types, which are distinguished by:

- length (1, 3, or 5 time slots depending on required payload size)
- forward error correction (optionally reducing the data rate in favour of reliability)
- modulation (EDR - enhanced data rate - packets allow up to triple data rate by using a different RF modulation for the payload)

A connection must be explicitly set up and accepted between two devices before packets can be transferred.

ACL packets are retransmitted automatically if unacknowledged, allowing for correction of a radio link that is subject to interference. For isochronous data, the number of retransmissions can be limited by a flush timeout; but without using L2PLAY retransmission and flow control mode or EL2CAP, a higher layer must handle the packet loss.

ACL links are disconnected if there is nothing received for the supervision timeout period; the default timeout is 20 seconds, but this may be modified by the master.

Synchronous connection-oriented (SCO) link

The type of radio link used for voice data. An SCO link is a set of reserved timeslots on an existing ACL link. Each device transmits encoded voice data in the reserved timeslot. There are no retransmissions, but forward error correction can be optionally applied. SCO packets may be sent every 1, 2 or 3 timeslots.

Enhanced SCO (eSCO) links allow greater flexibility in setting up links: they may use retransmissions to achieve reliability, allow a wider variety of packet types, and greater intervals between packets than SCO, thus increasing radio availability for other links.

Link management protocol (LMP)

Used for control of the radio link between two devices, handling matters such as link establishment, querying device abilities and power control. Implemented on the controller.

Host/controller interface (HCI)

Standardized communication between the host stack (e.g., a PC or mobile phone OS) and the controller (the Bluetooth IC). This standard allows the host stack or controller IC to be swapped with minimal adaptation.

There are several HCI transport layer standards, each using a different hardware interface to transfer the same command, event and data packets. The most commonly used are USB (in PCs) and UART (in mobile phones and PDAs).

In Bluetooth devices with simple functionality (e.g., headsets), the host stack and controller can be implemented on the same microprocessor. In this case the HCI is optional, although often implemented as an internal software interface.

Low Energy Link Layer (LE LL)

This is the LMP equivalent for Bluetooth Low Energy (LE), but is simpler. It is implemented on the controller and manages advertisement, scanning, connection and security from a low-level, close to the hardware point of view.

Host stack

Logical link control and adaptation protocol (L2CAP)

L2CAP is used within the Bluetooth protocol stack. It passes packets to either the Host Controller Interface (HCI) or on a hostless system, directly to the Link Manager.

L2CAP's functions include:

- Multiplexing data between different higher layer protocols.
- Segmentation and reassembly of packets.
- Providing one-way transmission management of multicast data to a group of other Bluetooth devices.
- Quality of service (QoS) management for higher layer protocols.

L2CAP is used to communicate over the host ACL link. Its connection is established after the ACL link has been set up.

In basic mode, L2CAP provides packets with a payload configurable up to 64 kB, with 672 bytes as the default MTU, and 48 bytes as the minimum mandatory supported MTU. In retransmission and flow control modes, L2CAP can be configured for reliable or isochronous data per channel by performing retransmissions and CRC checks. Reliability in either of these modes is optionally and/or additionally guaranteed by the lower layer Bluetooth BDR/EDR air interface by configuring the number of retransmissions and flush timeout (time after which the radio will flush packets). In-order sequencing is guaranteed by the lower layer.

The EL2CAP specification adds an additional *enhanced retransmission mode* (ERTM) to the core specification, which is an improved version of retransmission and flow control modes. ERTM is required when using an AMP, such as 802.11abgn.

Bluetooth network encapsulation protocol (BNEP)

BNEP is used for delivering network packets on top of L2CAP. This protocol is used by the *personal area networking (PAN)* profile. BNEP performs a similar function to Subnetwork Access Protocol (SNAP) in Wireless LAN.

In the protocol stack, BNEP is bound to L2CAP

Radio frequency communication (RFCOMM)

The Bluetooth protocol RFCOMM is a simple set of transport protocols, made on top of the L2CAP protocol, providing emulated RS-232 serial ports (up to sixty simultaneous connections to a Bluetooth device at a time). The protocol is based on the ETSI standard TS 07.10.

RFCOMM is sometimes called *serial port emulation*. The Bluetooth *serial port profile* is based on this protocol.

RFCOMM provides a simple reliable data stream to the user, similar to TCP. It is used directly by many telephony related profiles as a carrier for AT commands, as well as being a transport layer for OBEX over Bluetooth.

Many Bluetooth applications use RFCOMM because of its widespread support and publicly available API on most operating systems. Additionally, applications that used a serial port to communicate can be quickly ported to use RFCOMM

In the protocol stack, RFCOMM is bound to L2CAP.

Service discovery protocol (SDP)

Used to allow devices to discover what services each other support, and what parameters to use to connect to them. For example, when connecting a mobile phone to a Bluetooth headset, SDP will be used to determine which Bluetooth profiles are supported by the headset (*headset profile*, *hands free profile*, *advanced audio distribution profile*, etc.) and the protocol multiplexor settings needed to connect to each of them. Each service is identified by a Universally Unique Identifier (UUID), with official services (Bluetooth profiles) assigned a short form UUID (16 bits rather than the full 128)

In the protocol stack, SDP is bound to L2CAP.

Telephony control protocol (TCP)

Also referred to as *telephony control protocol specification binary* (TCS binary)

Used to set up and control speech and data calls between Bluetooth devices. The protocol is based on the ITU-T standard Q.931, with the provisions of Annex D applied, making only the minimum changes necessary for Bluetooth.

TCP is used by the *intercom* (ICP) and *cordless telephony* (CTP) profiles.

Audio/video control transport protocol (AVCTP)

Used by the remote control profile to transfer AV/C commands over an L2CAP channel. The music control buttons on a stereo headset use this protocol to control the music player

In the protocol stack, AVCTP is bound to L2CAP.

Audio/video data transport protocol (AVDTP)

Used by the advanced audio distribution profile to stream music to stereo headsets over an L2CAP channel. Intended to be used by video distribution profile.

In the protocol stack, AVDTP is bound to L2CAP.

Object exchange (OBEX)

Object exchange (OBEX; also termed *IrOBEX*) is a communications protocol that facilitates the exchange of binary objects between devices. It is maintained by the Infrared Data Association but has also been adopted by the Bluetooth Special Interest Group and the SyncML wing of the Open Mobile Alliance (OMA).

In Bluetooth, OBEX is used for many profiles that require simple data exchange (e.g., object push, file transfer, basic imaging, basic printing, phonebook access, etc.).

In the protocol stack, OBEX is bound to RFComm.

Low Energy Attribute Protocol (ATT)

Similar in scope to SDP but specially adapted and simplified for Low Energy Bluetooth. It allows a client to read and/or write certain attributes exposed by the server in a non-complex, low-power friendly manner.

In the protocol stack, ATT is bound to L2CAP.

Low Energy Security Manager Protocol (SMP)

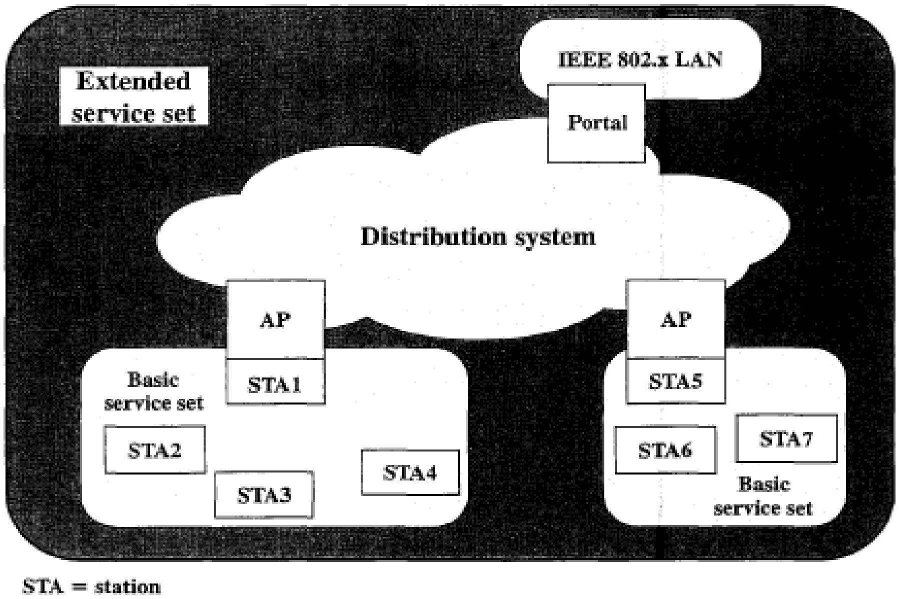
This is used by Bluetooth Low Energy Implementations for pairing and transport specific key distribution.

In the protocol stack, SMP is bound to L2CAP

Q 40) Discuss the architecture and the services provided by IEEE 802.11
Ans:

In 1990, the IEEE 802 Committee formed a new working group, IEEE 802.11, Specifically devoted to wireless LANs, with a charter to develop a MAC protocol and physical medium specification.

Architecture of IEEE 802.11:



The smallest building block of a wireless LAN is a basic service set (BSS), which consists of some number of stations executing the same MAC protocol and competing for access to the same shared wireless medium.

A BSS may be isolated or it may connect to a backbone distribution system (DS) through an access point (AP). The AP functions as a bridge and a relay point. In a BSS, client stations do not communicate directly with one another. Rather, if one station in the BSS wants to communicate with another station in the same BSS, the MAC frame is first sent from the originating station to the AP, and then from the AP to the destination station.

Similarly, a MAC frame from a station in the BSS to a remote station is sent from the local station to the AP and then relayed by the AP over the DS on its way to the destination station. The BSS generally corresponds to what is referred to as a cell in the literature. The DS can be a switch, a wired network, or a wireless network. When all the stations in the BSS are mobile stations, with no connection to Other BSSs, the BSS is called an independent BSS (IBSS). An IBSS is typically an adhoc network. In an IBSS, the stations all communicate directly, and no AP is involved. A simple configuration is shown in Figure, in which each station belongs to a single BSS; that is, each station is within wireless range only of other stations within the same BSS. It is also possible for two BSSs to overlap geographically, so that a single station could participate in more than one BSS. Further, the association between a station and a BSS is dynamic. Stations may turn off, come within range, and go out of range.

An **extended service set (ESS)** consists of two or more basic service sets interconnected by a distribution system. Typically, the distribution system is a wired backbone LAN but can be any communications network.

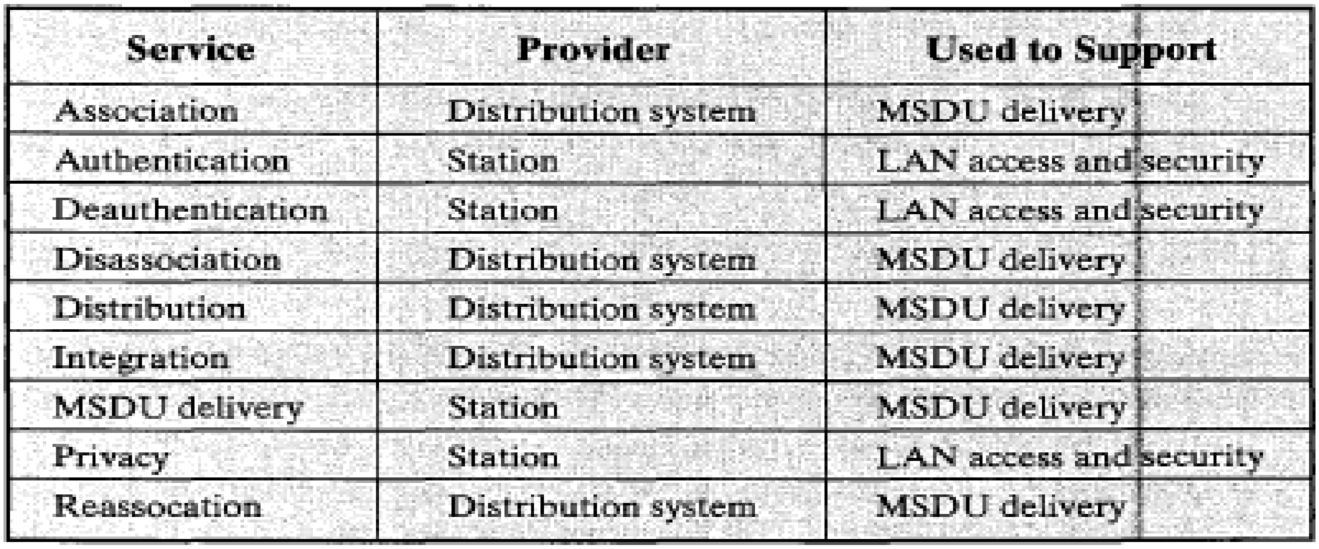
The extended service set appears as a single logical LAN to the logical link control (LLC) level. Figure indicates that an access point (AP) is implemented as part of a station; the AP is the logic within a station that provides access to the DS by providing DS services in addition to acting as a station. To integrate the IEEE 802.11 architecture with a traditional wired LAN, a **portal** is used. The portal logic is implemented in a device, such as a bridge or router, that is part of the wired LAN and that is attached to the DS.

IEEE 802.11 Services:

IEEE 802.11 defines nine services that need to be provided by the wireless LAN to provide functionality equivalent to that which is inherent to wired LANs. The service provider can be either the station or the distribution system (DS). Station services are implemented in every 802.11 station, including access point (AP) stations. Distribution services are provided between basic service sets (BSSs); these services may be implemented in an AP or in another special purpose device attached to the distribution system.

Three of the services are used to control IEEE 802.11 LAN access and confidentiality. Six of the services are used to support delivery of MAC service data units (MSDUs) between stations.

The MSDU is the block of data passed down from the MAC user to the MAC layer; typically this is a LLC PDU If the MSDU is too large to be transmitted in a single MAC frame, it may be fragmented and transmitted in a series of MAC frames



Service	Provider	Used to Support
Association	Distribution system	MSDU delivery
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Disassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery
Privacy	Station	LAN access and security
Reassocation	Distribution system	MSDU delivery

-- ----------------

Distribution of Messages within a DS : The two services involved with the distribution of messages within a DS are distribution and integration. Distribution is the primary service used by stations to exchange MAC frames when the frame must traverse the DS to get from a station in one BSS to a station in another BSS. If the two stations that are communicating are within the same BSS, then the distribution service logically goes through the single AP of that BSS.

The **integration** service enables transfer of data between stations on an IEEE 802.11 LAN and a station on an integrated IEEE 802.x LAN. The term *integrated* refers to a wired LAN that is physically connected to the DS and whose stations may be logically connected to an IEEE 802.11 LAN via the integration service. The integration service takes care of any address translation and media conversion logic required for the exchange of data.

Association-related Service: The primary purpose of the MAC layer is to transfer MSDUs between MAC entities; this purpose is fulfilled by the distribution service. For that service to function, it requires information about stations within the ESS, which is provided by the association-related services. Before the distribution service can deliver data to or accept data from a station, that station must be *associated.*
Mobility: The standard defines three transition types based on mobility:

No transition: A station of this type is either stationary or moves only within the direct communication range of the communicating stations of a single BSS.

BSS transition: This is defined as a station movement from one BSS to another BSS within the same ESS. In this case, delivery of data to the station requires that the addressing capability be able to recognize the new location of the station.

ESS transition: This is defined as a station movement from a BSS in one ESS to a BSS within another ESS. This case is supported only in the sense that the station can move. Maintenance of upper-layer connections supported by 802.11 cannot be guaranteed. In fact, disruption of service is likely to occur. To deliver a message within a DS, the distribution service needs to know where the destination station is located. Specifically, the DS needs to know the identity of the AP to which the message should be delivered in order for that message to reach the destination station. To meet this requirement, a station must maintain an association with the AP within its current BSS.
Three services relate to this requirement:

Association: Establishes an initial association between a station and an AP Before a station can transmit or receive frames on a wireless LAN, its identity and address must be known. For this purpose, a station must establish an association with an AP within a particular BSS.
The AP can then communicate this information to other APs within the ESS to facilitate routing and delivery of addressed frames.

Re-association: Enables an established association to be transferred from one AP to another, allowing a mobile station to move from one BSS to another.

Disassociation: A notification from either a station or an AP that an existing association is terminated. A station should give this notification before leaving an ESS or shutting down.

However, the MAC management facility protects itself against stations that disappear without notification.
Access and Privacy Services There are two characteristics of a wired LAN those are not inherent in a wireless LAN.
1. In order to transmit over a wired LAN, a station must be physically connected to the LAN. On the other hand, with a wireless LAN, any station within radio range of the other devices on the LAN can transmit. In a sense, there is a form of authentication with a wired LAN, in that it requires some positive and presumably observable action to connect a station to a wired LAN.

2. Similarly, in order to receive a· transmission from a station that is part of a wired LAN, the receiving station must also be attached to the wired LAN. On the other hand, with a wireless LAN, any station within radio range can receive. Thus, a wired LAN provides a degree of privacy, limiting reception of data to stations connected to the LAN. IEEE 802.11 defines three services that provide a wireless LAN with these two features:

• Authentication: Used to establish the identity of stations to each other. In a wired LAN, it is generally assumed that access to a physical connection conveys authority to connect to the LAN. This is not a valid assumption for a wireless LAN, in which connectivity is achieved simply by having an attached antenna that is properly tuned. The authentication service is used by stations to establish their identity with stations they wish to communicate with. IEEE 802.11 supports several authentication schemes and allows for expansion of the functionality of these schemes. The standard does not mandate any particular authentication scheme, which could range from relatively unsecure handshaking to public key encryption Schemes. However, IEEE 802.11 requires mutually acceptable, successful Authentication before a station can establish an association with an AP.

• De-authentication: This service is invoked whenever an existing authentication is to be terminated.

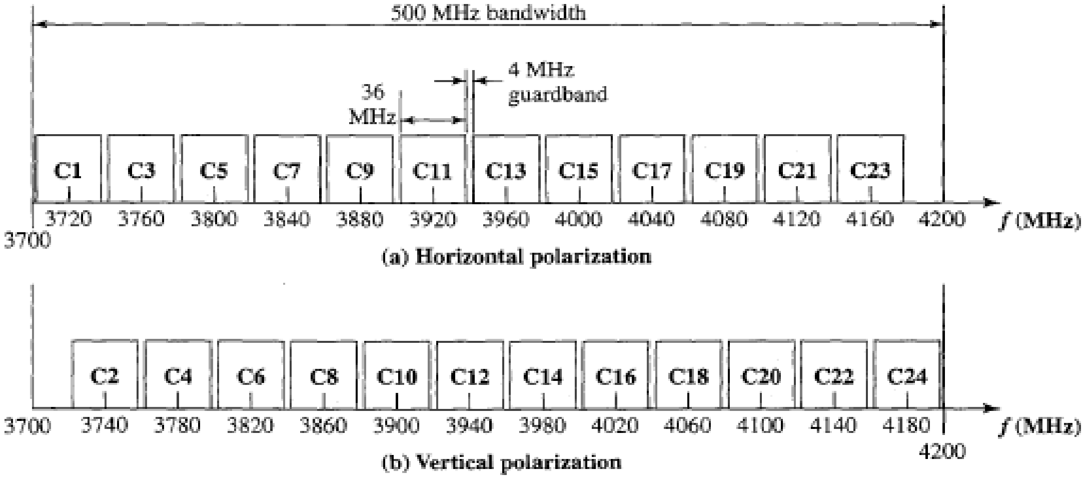
• Privacy: Used to prevent the contents of messages from being read by other than the intended recipient. The standard provides for the optional use of encryption to assure privacy. These are the services provided by IEEE 802.11

Q 41) Explain how the capacity of a satellite is allocated using frequency division.

Ans:

For each of the channels of satellite, there is a capacity allocation task to be performed. The cost-effective use of the satellite requires that each channel be shared by many users. Hence, the task is fundamentally one of multiplexing. In some cases, the allocation is carried out by a centralized control, usually by the satellite; but in other cases, the allocation is a distributed function.

Frequency Division Multiplexing:
In this, the overall capacity of a communications satellite is divided into a number of channels. This is a top level of FDM, with further capacity allocation carried out within each channel. Following Figure is an example of an FDM scheme, which is typical of GEO communications satellites; this particular allocation is used in the Galaxy satellites from PanAmSat.3 The satellite uses C band frequencies and provides a 500-MHz bandwidth, which is broken up into 24 40-MHz channels.



Typical Satellite Transponder Frequency Plan for the Downlink Channels (for the uplink plan, and 2225 MHz to the numbers given above)

The satellite is able to squeeze 24 channels into the 500 MHz by means of **frequency** reuse:
Each frequency assignment is used by two carriers with orthogonal polarization.
Each 40-MHz channel includes a 4-MHz guard band, so each channel is actually 36 MHz wide.
When used in a point-to-point configuration each channel could be used for one of a number of alternative purposes.
Examples include

- 1200 voice-frequency (VF) voice channels
- One 50-Mbps data stream
- 16 channels of 1.544 Mbps each
- 400 channels of 64 kbps each
- 600 channels of 40 kbps each
- One analog video signal
- Six to nine digital video signals

Frequency Division Multiple Access

The satellite is used as in intermediate device providing, in effect, a point-to-point link between two earth stations.

Because of the wide area coverage of the satellite, this is not necessarily the case to be divided using FDM into a number of smaller channels, each of which uses FM.

Each of the smaller channels in turn carries a number of voice frequency (VF) signals using FDM. The ability of multiple earth stations to access the same channel is referred to as FDMA.

The number of sub channels provided within a satellite channel via FDMA is limited by three factors:

- Thermal noise
- Intermodulation noise
- Crosstalk

The first two factors work in opposite directions. With too little signal strength, the transmitted signal will be corrupted by background noise.

With too much signal strength, nonlinear effects in the satellite's amplifiers result in high intermodulation noise.

Crosstalk stems from a desire to increase capacity by reusing frequencies and limits but does not eliminate that practice.

A frequency band can be reused if antennas that can radiate two polarized signals of the same frequency (co-channels) in orthogonal planes are employed.

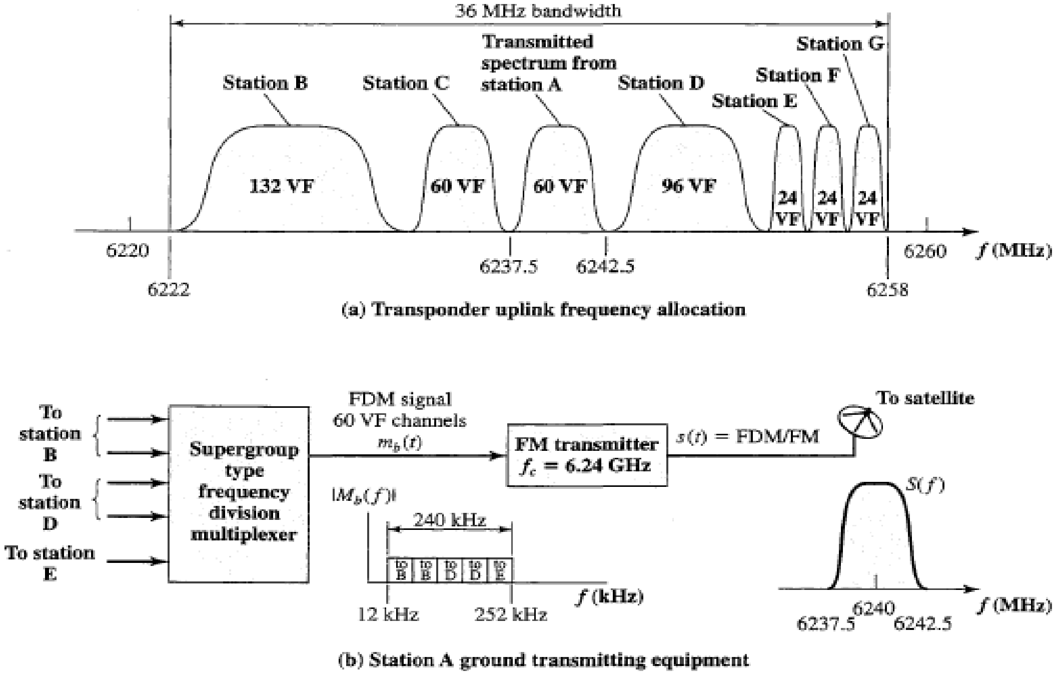
Again if signal strength is too high, co-channel interference becomes significant.

Two forms of FDMA are possible:

- Fixed-assignment **multiple** access (FAMA): The assignment of capacity within the overall satellite channel is distributed in a fixed manner among multiple stations. This often results in significant underuse of the capacity, as demand may fluctuate.

- Demand-assignment **multiple** access (DAMA): The capacity assignment is changed as needed to respond optimally to demand changes among the multiple stations.

FAMA-FDMA :



(a) Transponder uplink frequency allocation

(b) Station A ground transmitting equipment

Fixed-Assignment FDMA Format for Satellite Communication [COUC01]

FAMA-FDMA Figure is a specific example of FAMA-FDMA, with seven earth stations sharing the 36-MHz uplink capacity; a similar downlink diagram can be drawn.

Station A is assigned the 5-MHz bandwidth from 6237.5 to 6242.5 MHz, in which it can transmit 60 VF channels using FDM-FM. That is, FDM is used to carry the 60 channels, and FM is used to modulate the channels onto the carrier frequency of 6240 MHz.

The figure indicates that station A has traffic for other stations as follows: 24 channels to B, 24 channels to D, and 12 channels to E.

The remaining spectrum of the 36-MHz channel is divided among the other earth stations according to their traffic needs.

This example brings up several instructive points:

• The scheme illustrates both FAMA and FDMA. The term *FAMA* refers to the fact that the logical links between stations are preassigned. Thus in Figure it appears to station A that it has three direct point-to-point links, one each to B (24 channels), D (24 channels), and E (12 channels). The term *FDMA* refers to the fact that multiple stations are accessing the satellite link by using different frequency bands.

• Although an earth station may transmit only one carrier up to the satellite able to receive at least one carrier for each remote location with which it wishes to communicate (e.g., A must receive three carriers, parts of the transmission of B, D, and E).

• The satellite performs no switching function. Although it is receiving portions of the 36-MHz channel from various sources, it simply accepts signals across that spectrum, translates them to the 4-Ghz band, and retransmits them.

• Considerable bandwidth is used This is due to the use of FM (rather than AM) to maintain signal over the long distance of the satellite link and to minimize satellite power requirements.

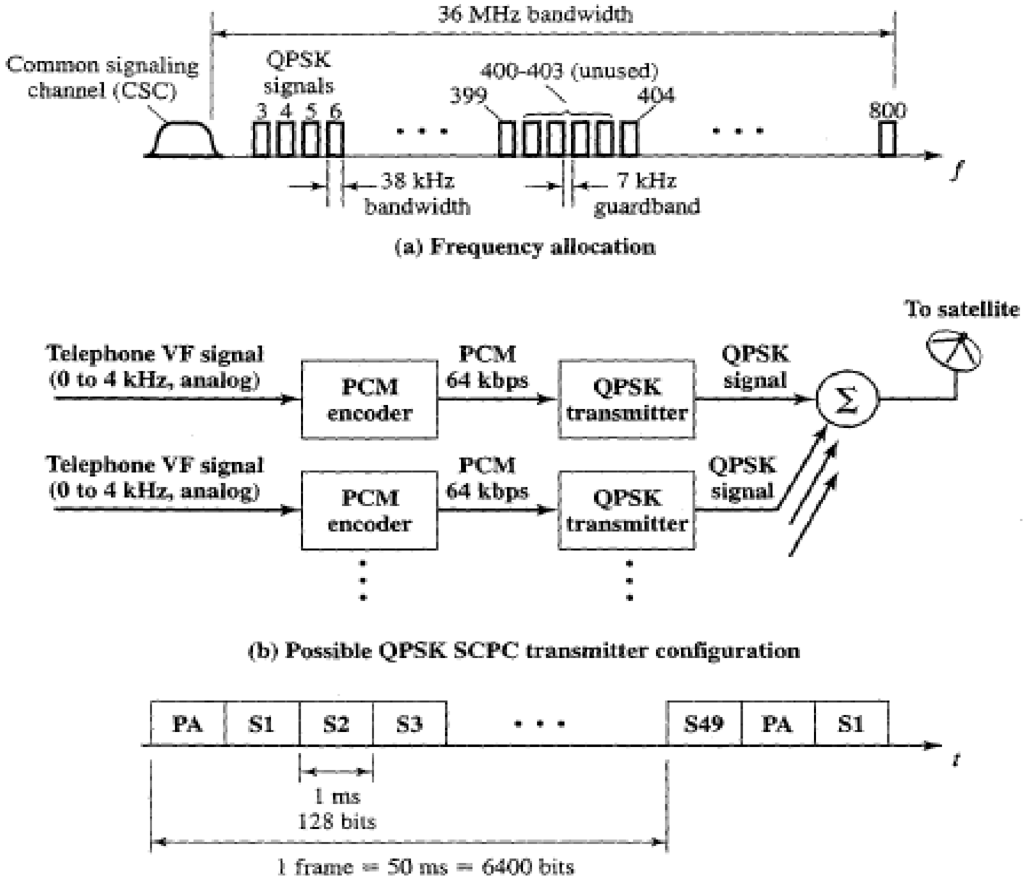
DAMA-FDMA :

The FAMA-FDMA scheme just described is not efficient. Typically, in the C band, each channel has a usable bandwidth of 36 MHz.

One INTELSAT FDMA scheme divides this into 7 5-MHz blocks, each of which carries a group of 60 VF channels, for a total of 420 channels.

Our example also carries 420 channels. When the bandwidth is divided into 14 2.5-MHz subchannels, two groups of 48 VF channels can be carried in each channel for a total of 336 channels.

It turns out to be more efficient to avoid groupings altogether and simply to divide the 36-MHz bandwidth into individual VF channels. This technique is known as single channel per carrier (SCPC).



(a) Frequency allocation

(b) Possible QPSK SCPC transmitter configuration

(c) TDMA CSC frame format

--SCPC is currently provided in the C band. A single 36-MHz channel is subdivided into 800 45-kHz analog channels, each dedicated to a simplex VF link, using FM.

There is also digital SCPC, using QPSK, which provides 64-kbps service in the same 45-kHz bandwidth, enough for digitized voice. With FAMA, pairs of channels (for full duplex) are assigned to pairs of earth stations.

Typically, each earth station is multiplexed, supporting a small number of user stations. With multiple user stations per earth station, a high degree of connectivity is achieved even with FAMA. As with conventional FDMA, the satellite accepts frequencies across the entire 36-MHz channel, translates them to the 4-GHz band, and broadcasts the channel to all stations.

SCPC is attractive for remote areas where there are few user stations near each site. Whereas FDMA is used as a trunk facility in the long-haul telecommunication system, SCPC provides direct end-user service.

Although SCPC is more efficient of bandwidth than FDMA, it does suffer from the inefficiency of fixed assignment.

This is especially unsuitable in very remote areas, where it is typical that each earth station serves one or a very few user stations.

To achieve greater efficiency, DAMA is used. With DAMA, the set of subchannels in a channel is treated as a pool of available links.

To establish a full-duplex link between two earth stations, a pair of subchannels is dynamically assigned on demand.

The first commercially available DAMA SCPC system was SPADE (single channel per carrier, pulse code modulation, multiple-access, demand-assignment equipment).

Q 44) Explain Bluetooth protocol stack in detail. Give examples of the applications it can handle.

Ans:
Bluetooth provides a universal short-range wireless capability. Using the 2.4-GHz band, available globally for unlicensed low-power uses, two Bluetooth devices within 10m of each other can share up to 720 kbps of capacity. Bluetooth is defined as a layered protocol architecture consisting of core protocols, cable replacement and telephony control protocols, and adopted protocols. The core protocols form a five-layer stack consisting of the following elements:

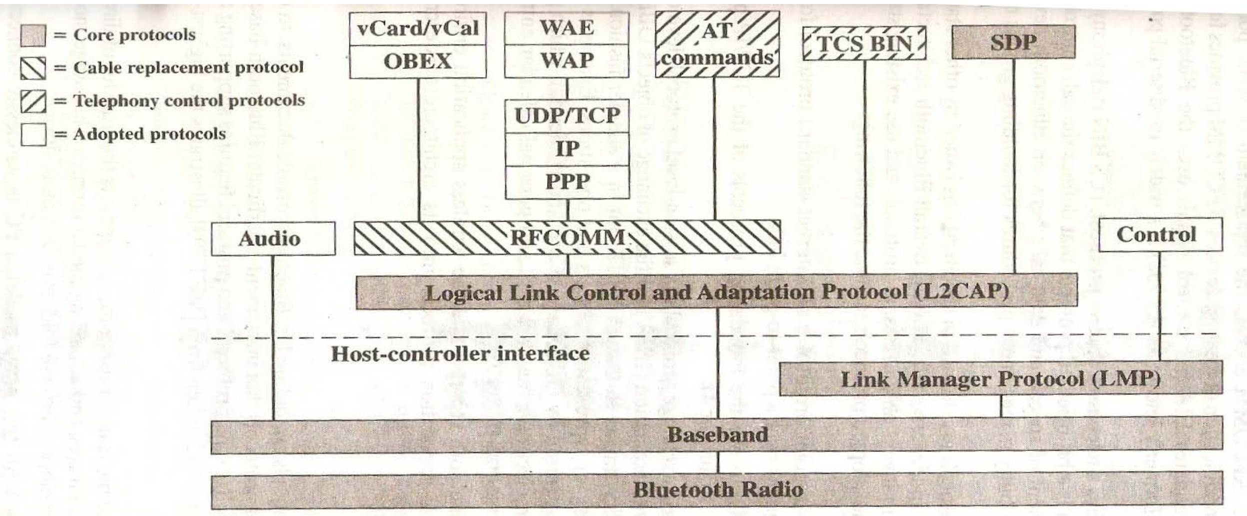
- Radio: specifies details of the air interface, including frequency, the use of frequency hopping, modulation scheme, and transmit power.
- Baseband: concerned with connection establishment within a piconet, addressing, packet format, timing, and power control.
- Link manager protocol(LMP): Responsible for link setup between Bluetooth devices and ongoing link management. This includes security aspects such as authentication and encryption, plus the control and negotiation of baseband packet sizes.
- Logical link control and adaptation protocol (L2CAP): adapts upper-layer protocols to the baseband layer. L2CAP provide both connectionless and connection-oriented services.
- Services discovery protocol (SDP): Device information, services, and the characteristics of the services can be queried to enable the establishment of a connection between two or more Bluetooth devices.

RFCOMM is the cable replacement protocol included in the Bluetooth specification. RFCOMM presents a virtual serial port that is designed to make replacement of cable technologies as transparent as possible. Serial ports are one of the most common types of communications interfaces used with computing and communications devices. Hence, RFCOMM enables the replacement of serial port cables with minimum of modification of existing devices. RFCOMM provides for binary data transport and emulates EIA-232 control signals over the Bluetooth baseband layer. EIA-232 is widely used serial port interface standard.

Bluetooth specifies a telephony control protocol. TCS BIN (telephony control specification-binary) is a bit-oriented protocol that defines the call control signaling for the establishment if speech and data calls between Bluetooth devices, in addition, it defines mobility management procedures for handling groups of Bluetooth TCS devices.

The adopted protocols are defined in specifications issued by other standards-making organizations and incorporated into overall Bluetooth architecture. The Bluetooth strategy is to invent only necessary protocols and use existing standards whenever possible. The adopted protocols include the following:

- PPP: the point-to-point protocol is an Internet standard protocol for transporting IP datagrams over a point-to-point link.
- TCP/UDP/IP: These are the foundation protocols of the TCP/IP protocol suite.
- OBEX: The object exchange protocol is a session-level protocol developed by the Infrared Data Association(IDA) for the exchange of objects. OBEX provides a model for representation of objects and operations. Examples of content formats transferred by OBEX are vCard and vCalendar, which provide the format of an electronic business card and personal calendar entries and scheduling information, respectively.
- WAE/WAP: Bluetooth incorporates the wireless application environment and the wireless application protocol into its architecture.


▨ = Core protocols
▧ = Cable replacement protocol
▨ = Telephony control protocols
□ = Adopted protocols
vCard/vCal
OBEX
WAE
WAP
AT commands
TCS BIN
SDP
UDP/TCP
IP
PPP
Audio
RFCOMM
Control
Logical Link Control and Adaptation Protocol (L2CAP)
Host-controller interface
Link Manager Protocol (LMP)
Baseband
Bluetooth Radio

AT	= attention sequence (modem prefix)	TCS BIN	= telephony control specification—binary
IP	= Internet Protocol	UDP	= User Datagram Protocol
OBEX	= Object Exchange Protocol	vCal	= virtual calendar
PPP	= Point-to-Point Protocol	vCard	= virtual card
RFCOMM	= radio frequency communications	WAE	= wireless application environment
SDP	= Service Discovery Protocol	WAP	= Wireless Application Protocol
TCP	= Transmission Control Protocol		

Fig. Bluetooth protocol stack.

Bluetooth provides support for three general application areas using short-range wireless connectivity:

- Connection of peripheral devices: Today, most devices are connected to a desktop computer via wires (e.g., keyboard, mouse, joystick, headset, speakers).This type of connection has several disadvantages: each device has its own type of cable, different plugs are needed, wires block office space. In a wireless network, no wires are needed for data transmission. However, batteries now have to replace the power supply, as the wires not only transfer data but also supply the peripheral devices with power.

- Support of ad-hoc networking: Imagine several people coming together, discussing issues, exchanging data (schedules, sales figures etc.). For instance, students might join a lecture, with the teacher distributing data to their personal digital assistants (PDAs). Wireless networks can support this type of interaction; small devices might not have WLAN adapters following the IEEE 802.11 standard, but cheaper Bluetooth chips built in.

- Bridging of networks: Using wireless piconets, a mobile phone can be connected to a PDA or laptop in a simple way. Mobile phones will not have full WLAN adapters built in, but could have a Bluetooth chip. The mobile phone can then act as a bridge between the local piconet and, e.g., the global GSM network (see Figure 7.40). For instance, on arrival at an airport, a person's mobile phone could receive e-mail via GSM and forward it to the laptop which is still in a suitcase. Via a piconet, a fileserver could update local information stored on a laptop or PDA while the person is walking into the office.

Q 45) Discuss TDMA, FDMA and CDMA access techniques. Which access technique requires least power and yet gives better noise immunity?

Ans:

TDMA (Time Division Multiple Access):

Time division multiple access (TDMA) offers flexible scheme, which comprises all technologies that allocate certain time slots for communication, i.e., controlling TDM. Now tuning in to a certain frequency is not necessary, i.e., the receiver can stay at the same frequency the whole time. Using only one frequency, and thus very simple receivers and transmitters, many different algorithms exist to control medium access. As already mentioned, listening to different frequencies at the same time is quite difficult, but listening to many channels separated in time at the same frequency is simple. Almost all MAC schemes for wired networks work according to this principle, e.g., Ethernet, Token Ring, ATM etc. Synchronization between sender and receiver has to be achieved in the time domain. This can be done by using a fixed pattern, i.e., allocating a certain time slot for a channel, or by using a dynamic allocation scheme. Dynamic allocation schemes require identification for each transmission as this is the case for typical wired MAC schemes or the transmission has to be announced beforehand. MAC addresses are quite often used as identification. This enables a receiver in a broadcast medium to recognize if it really is the intended receiver of a message. Fixed schemes do not need identification, but are not as flexible considering varying bandwidth requirements.

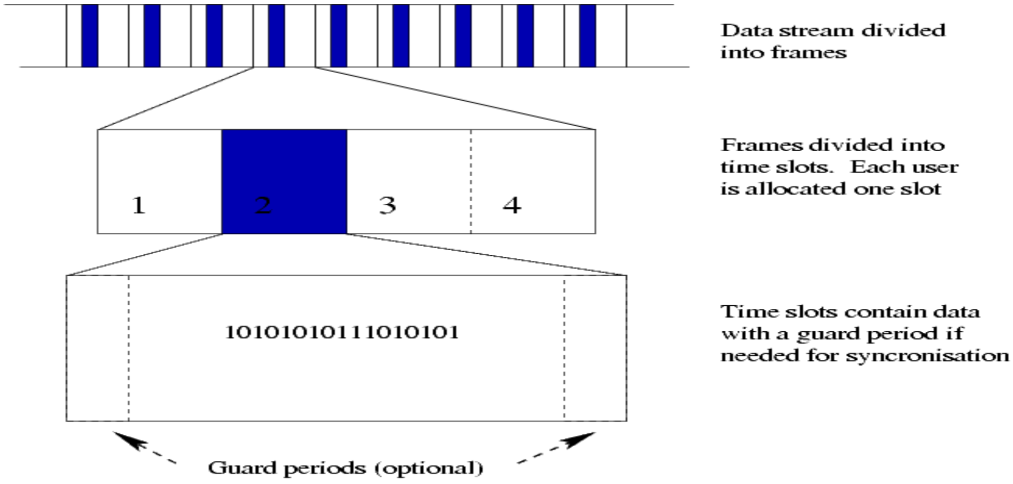

Data stream divided into frames
Frames divided into time slots. Each user is allocated one slot
1
2
3
4
10101010111010101
Time slots contain data with a guard period if needed for syncronisation
Guard periods (optional)

Fig. TDMA frame structure

Frequency Division Multiple Access (FDMA):

Frequency division multiple access (FDMA) comprises all algorithms allocating frequencies to transmission channels according to the frequency division multiplexing (FDM) scheme. Allocation can either be fixed or dynamic. Channels can be assigned to the same frequency at all times, i.e., pure FDMA, or change frequencies according to a certain pattern, i.e., FDMA combined with TDMA. FDM is often used for simultaneous access to the medium by base station and mobile station in cellular networks. Here the two partners typically establish a duplex channel, i.e., a channel that allows for simultaneous transmission in both directions. The two directions, mobile station to base station and vice versa are now separated using different frequencies. This scheme is then called frequency division duplex (FDD). Again, both partners have to know the frequencies in advance; they cannot just listen into the medium. The two frequencies are also known as uplink, i.e., from mobile station to base station or from ground control to satellite, and as downlink, i.e., from base station to mobile station or from satellite to ground control.

As for example FDM and FDD, Figure shows the situation in a mobile phone network based on the GSM standard for 900 MHz. The basic frequency allocation scheme for GSM is fixed and regulated by national authorities. All uplinks use the band between 890.2 and 915 MHz, all downlinks use 935.2 to 960 MHz. According to FDMA, the base station, shown on the right side, allocates a certain frequency for up- and downlink to establish a duplex channel with a mobile phone. Up- and downlink have a fixed relation. If the uplink frequency is fu = 890 MHz + n·0.2 MHz, the downlink frequency is fd = fu + 45 MHz, i.e., fd = 935 MHz + n·0.2 MHz for a certain channel n. The base station selects the channel. Each channel (uplink and downlink) has a bandwidth of 200 kHz. This illustrates the use of FDM for multiple access (124 channels per direction are available at 900 MHz) and duplex according to a predetermined scheme.

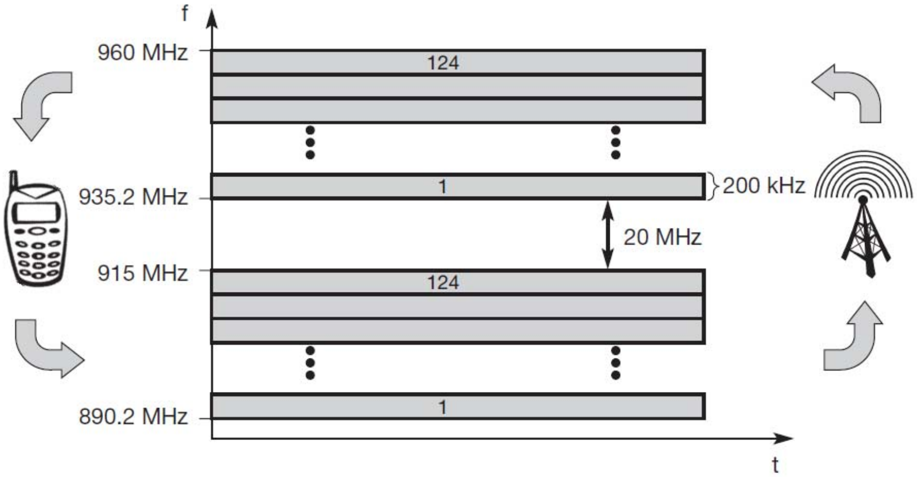


Fig. Frequency division multiplexing for multiple access

Code Division Multiple Access(CDMA):

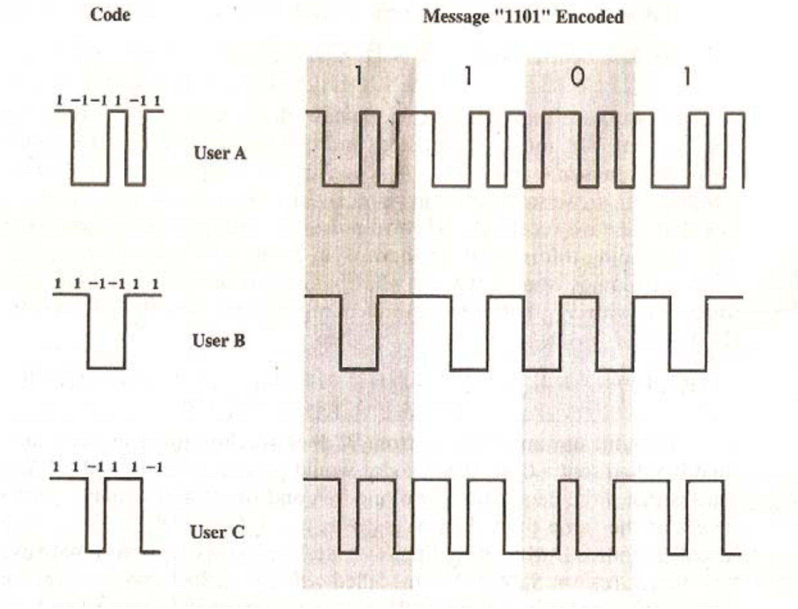


Fig. CDMA Example

CDMA is a multiplexing technique used with spread spectrum. The scheme works in the following manner. We start with a data signal with rate D, which we call the bit data rate. We break each bit into chips according to a fixed pattern that is specific to each user, called user's code. The new channel has a chip data rate of kD chips per second. As an illustration we consider a simple example with k=6. It is simplest to characterize a code as a sequence of 1s and -1s. Fig shows the codes for three users, A, B and C, each of which is communicating with the same base station receiver, R. Thus, the code for user A is c_A = <1,-1,-1,1,-1,1>, similarly, user B has code c_B = <1,1,-1,-1,1,1>, and user C has c_C = <1,1,-1,1,1,-1>.

Consider the case of user A communicating with the base station. The base station is assumed to know A's code. If a wants to send a 1bit, A transmits its code as a chip pattern <1,-1,-1,1,-1,1>. If a 0 is to be sent, A transmits the complement (1s and -1s reversed) of its code, <-1,1,1,-1,1,-1>. At the base station the receiver decodes the chip patterns. In our simple version, if the receiver R receives a chip pattern d = <d1,d2,d3,d4,d5,d6>, and the receiver is seeking to communicate with a user u so that it has at hand u's code,<c1,c2,c3,c4,c5,c6>, the receiver performs electronically the following decoding function:

$S_u(d)$ = (d1*c1)+(d2*c2)+(d3*c3)+(d4*c4)+(d5*c5)+(d6*c6)

The subscript u on S simply indicates that u is the user that we are interested in. let's suppose the user u is actually A and see what happens. If A sends a 1 bit, then d is <1,-1,-1,1,-1,1> and the preceding computation using S_A becomes

$S_A(1,-1,-1,1,-1,1) = [1*1]+[(-1)*(-1)]+[(-1)*(-1)]+[(-1)*(-1)]+[1*1] = 6$

If A sends a 0 bit that corresponds to d =<-1,1,1,-1,1,-1>, we get

$S_A(-1,1,1,-1,1,-1)= -6$

Also S_A is such that $-6 <= S_A(d) <= 6$.

If S_A produces a +6, we say that we have received a 0 bit from user A, otherwise, we assume that someone else is sending information or there is an error. If B sends a 1 bit, then
d = <1,1,-1,-1,1,1>. Then

$S_A(1,1,-1,-1,1,1) = 0$. Thus, the unwanted signal (from B) does not show up at all. You can easily verify that if B had sent a 0 bit, the decoder would produce a value of 0 for S_A again. This means that if the decoder is linear and if A and B transmit signals s_A and s_B, respectively, at the same time, then $S_A(s_A + s_B)=S_A(s_A)+S_A(s_B)=S_A(s_A)$ since the decoder ignores B when it is using A's code. The codes of A and B that have the property that $S_A(c_B) = S_B(c_A) = 0$ are called orthogonal.

The CDMA receiver can filter out the contribution from unwanted users or they appear as low-level noise. However, if there are contribution many users competing for the channel with user the receiver is trying to listen to, or if the signal power of one or more competing signals is too high, perhaps because it is very near the receiver, the system breaks down. TDMA (Time Division Multiple Access) technique requires least power and yet gives better noise immunity

Q 47) Explain how the following impairments affect wireless communication: Attenuation, Noise, Atmospheric absorption, and Multipath fading.

Ans: With any communications system, the signal that is received will differ from the signal that is transmitted, due to various transmission impairments. Few of the impairments affecting wireless communication are:

- Attenuation
- Noise
- Atmospheric absorption
- Multipath fading

Attenuation

The strength of a signal falls off with distance over any transmission medium. For unguided media attenuation is a complex function of distance and the makeup of the atmosphere. Attenuation introduces three factors for the transmission engineer:

1. A received signal must have sufficient strength so that the electronic circuitry in the receiver can detect and interpret the signal.
2. The signal must maintain a level sufficiently higher than noise to be received without error.
3. Attenuation is greater at higher frequencies, causing distortion.

The first and second factors are dealt with by attention to signal strength and the use of amplifiers or repeaters. The third factor is known as attenuation distortion. Because the attenuation varies as a function of frequency, the received signal is distorted, reducing intelligibility. To overcome this problem, techniques are available for equalizing attenuation across a band of frequencies.

Noise

For any data transmission event, the received signal will consist of the transmitted signal, modified by the various distortions imposed by the transmission system, plus additional unwanted signals that are inserted somewhere between transmission and reception. These unwanted signals are referred to as noise.

Noise may be divided into four categories:

- Thermal noise - due to thermal agitation of electrons and is a function of temperature.
- Intermodulation noise - when signals at different frequencies share the same transmission medium.
- Crosstalk – an unwanted coupling between signal paths.
- Impulse noise – noncontinuous, consisting of irregular pulses or noise spikes of short duration and of relatively high amplitude.

Atmospheric absorption

An additional loss between the transmitting and receiving antennas is atmospheric absorption. Water vapor and oxygen contribute most attenuation. A peak attenuation occurs in the vicinity of 22GHz due to vapor. At frequencies below 15 GHz, the attenuation is less. The presence of oxygen results in an absorption peak in the vicinity of 60GHz but contributes less at frequencies below 30GHz. Rain and fog cause scattering of radio waves that results in attenuation. This can be a major cause of signal loss. Thus, in areas of significant precipitation, either path lengths have to be kept short or lower-frequency bands should be used.

Multipath fading

In wireless communications, 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.

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, delay and 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.

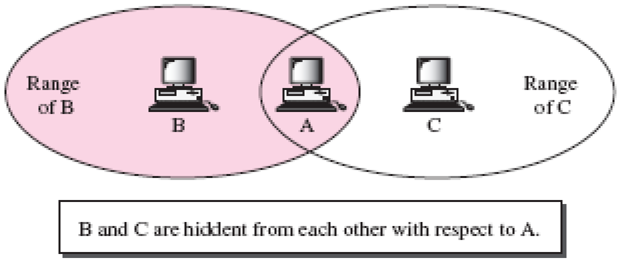
Q 48) Discuss the "Hidden Station problem" and "exposed station problem" in IEEE 802.11.How are they overcome?

Ans:

<u>Hidden Station Problem</u>:

Figure shows an example of the hidden station problem. Station B has a transmission range shown by the left oval (sphere in space); 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.

Figure 14.10 *Hidden station problem*



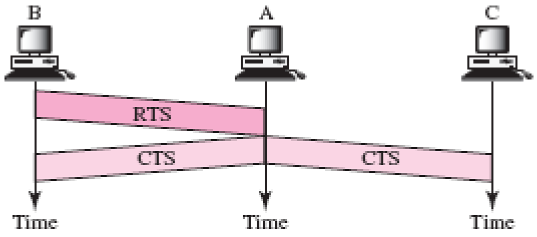
B and C are hiddent from each other with respect to A.

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) that we discussed earlier. Figure 14.11 shows that the RTS message from B reaches A, but not C. However, because both B and C are within the range of A, the CTS message, which contains the duration of data transmission from B to A reaches C. Station C knows that some hidden station is using the channel and refrains from transmitting until that duration is over.

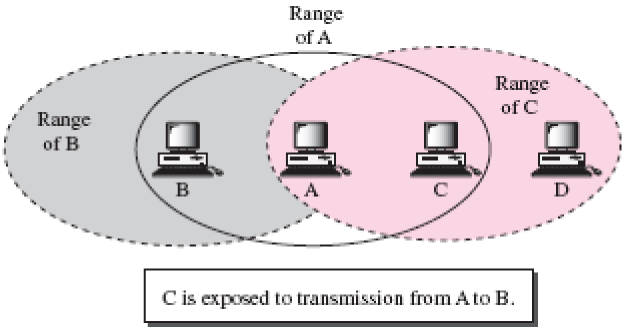
The CTS frame in CSMA/CA handshake can prevent collision from a hidden station.

Figure 14.11 *Use of handshaking to prevent hidden station problem*



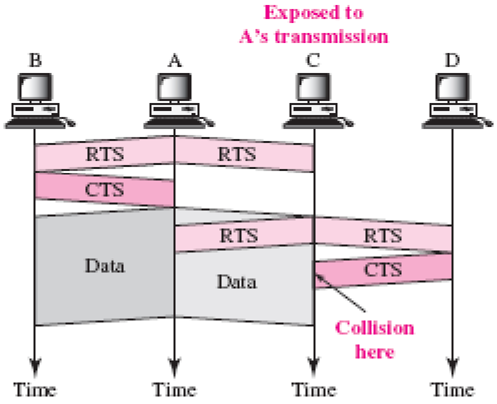
Exposed Station Problem: Now consider a situation that is the inverse of the previous one: the exposed station problem. In this problem a station refrains from using a channel when it is, in fact, available. In Figure 14.12, station A is transmitting to station B. Station C has some data to send to station 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.

Figure 14.12 *Exposed station problem*



The handshaking messages RTS and CTS cannot help in this case, despite what you might think. Station C hears the RTS from A, but does not hear the CTS from B. Station C, after hearing the RTS from A, can wait for a time so that the CTS from B reaches A; it then sends an RTS to D to show that it needs to communicate with D. Both stations B and A may hear this RTS, but station A is in the sending state, not the receiving state. Station B, however, responds with a CTS. The problem is here. If station A has started sending its data, station C cannot hear the CTS from station D because of the collision; it cannot send its data to D. It remains exposed until A finishes sending its data as Figure 14.13 shows.

Figure 14.13 *Use of handshaking in exposed station problem*



Q49. Suppose a transmitter produces 5 W of power-
a. Express transmit power in units of dBm and dBW
b. If the transmitter power in applied to unity gain antenna with 900MHz carrier frequency what is the received power in dBm at a free space distance of 100 m. Assume log 5= 0.7;log 9=0.9 for your calculation and use fixed free space loss of -147.56.

Answer –

a)
i) dBm or *decibel-milliwatt* is an electrical power unit in decibels (dB), referenced to 1 milliwatt (mW).
The power in decibel-milliwatts ($P_{(dBm)}$) is equal to the base 10 logarithm of the power in milliwatts ($P_{(mW)}$):
$P_{(dBm)} = 10 \cdot \log_{10}(P_{(mW)} / 1mW)$
Power produced by transmitter = 5W = 5000 mW

P(dBm)= 10 * log (5000 / 1)
= 10 * 3.69897
= 37 dBm

5 W = 37 dBm

ii) dBW or *decibel-watt* is a unit of power in decibel scale, referenced to 1 watt (W).
The power in decibel-watts ($P_{(dBW)}$) is equal to the base 10 logarithm of the power in watts ($P_{(W)}$):
$P_{(dBW)} = 10 \cdot \log_{10}(P_{(W)} / 1W)$
Power produced by transmitter = 5W

P(dBW)= 10 * log (5 / 1)
= 10 * 0.69897
= 7 dBW

5 W = 7 dBW

b)
Data given –
carrier frequency (f) = 900MHz
free space distance (d) =100 m.
log 5= 0.7
log 9=0.9
fixed free space loss of -147.56.
Signal power at transmitting antenna (Pt) = 37 dBm

Calculate : Signal power at receiving antenna (Pr) .

We know that , for the ideal isotropic antenna (unity gain antenna) , free space loss is ,

L_{dB} = 20 log(f) + 20 log(d) – 147.56 dB
= 20 log(900) + 20 log(100) – 147.56
= 20 * 2.9542 + 20 * 2 – 147.56
= 59.08 + 40 – 147.56
= 99.08 – 147.56
= 48.48 dB

We also have ,

L_{dB} = 10 log (Pt/Pr)
= 10 * (log Pt – log Pr)
48.48 = 10 * (log 37 – log Pr)
48.48 = 10 * (1.5682 – log Pr)
48.48 = 15.682 – 10 log Pr
48.48 – 15.682 = - 10 log Pr
32.798 = - 10 log Pr
Log Pr = - 32.798 / 10
Pr = $10^{-3.2798}$
Pr = 5.2504 * 10^{-4} dBm

Q 50) How the wireless media issues are addressed by WAE/WAP specification? Describe WSP and WTP in this context.

Ans: Wireless Application Environment

The WAE specifies an application framework for wireless devices such as mobile telephones, pagers, and PDAs. In essence, the WAE consists of tools and formats that are intended to ease the task of developing applications and devices supported by WAP. The major elements of the WAE model are as follows (Figure 1): _

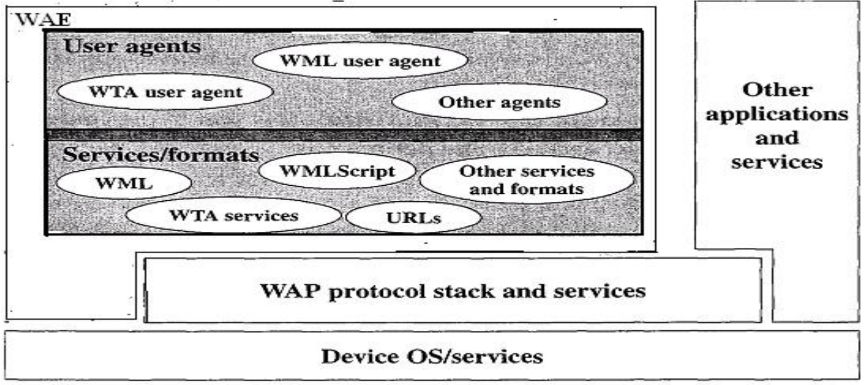


Fig.1.WAE Client Components

- WAE user agents: Software that executes in the user's wireless device and that provides specific functionality (e.g., display content) to the end user.
- Content generators: Applications (or services) on origin servers (e.g., CGI scripts) that produce standard content formats in response to requests from user agents in the mobile terminal. WAE does not specify any standard content generators but expects that there will be a variety available running on typical HTTP origin servers commonly used in WWW today.
- Standard content encoding: Defined to allow a WAE user agent (e.g., a browser) to conveniently navigate Web content.
- Wireless telephony applications (WTA): A collection of telephony-specific extensions for call and feature control mechanisms that provide authors advanced mobile network services. Using WTA, applications developers can use the micro browser to originate telephone calls and to respond to events from the telephone network.

Wireless Session Protocol

WSP provides applications with an interface for two session services. The connection oriented session service operates above the reliable transport protocol WTP, and the connectionless session service operates above the unreliable transport protocol WDP. In essence, WSP is based on HTTP with some additions and modifications to optimize its use over wireless channels. The principal limitations addressed are low data rate and susceptibility to loss of connection due to poor coverage or cell overloading.

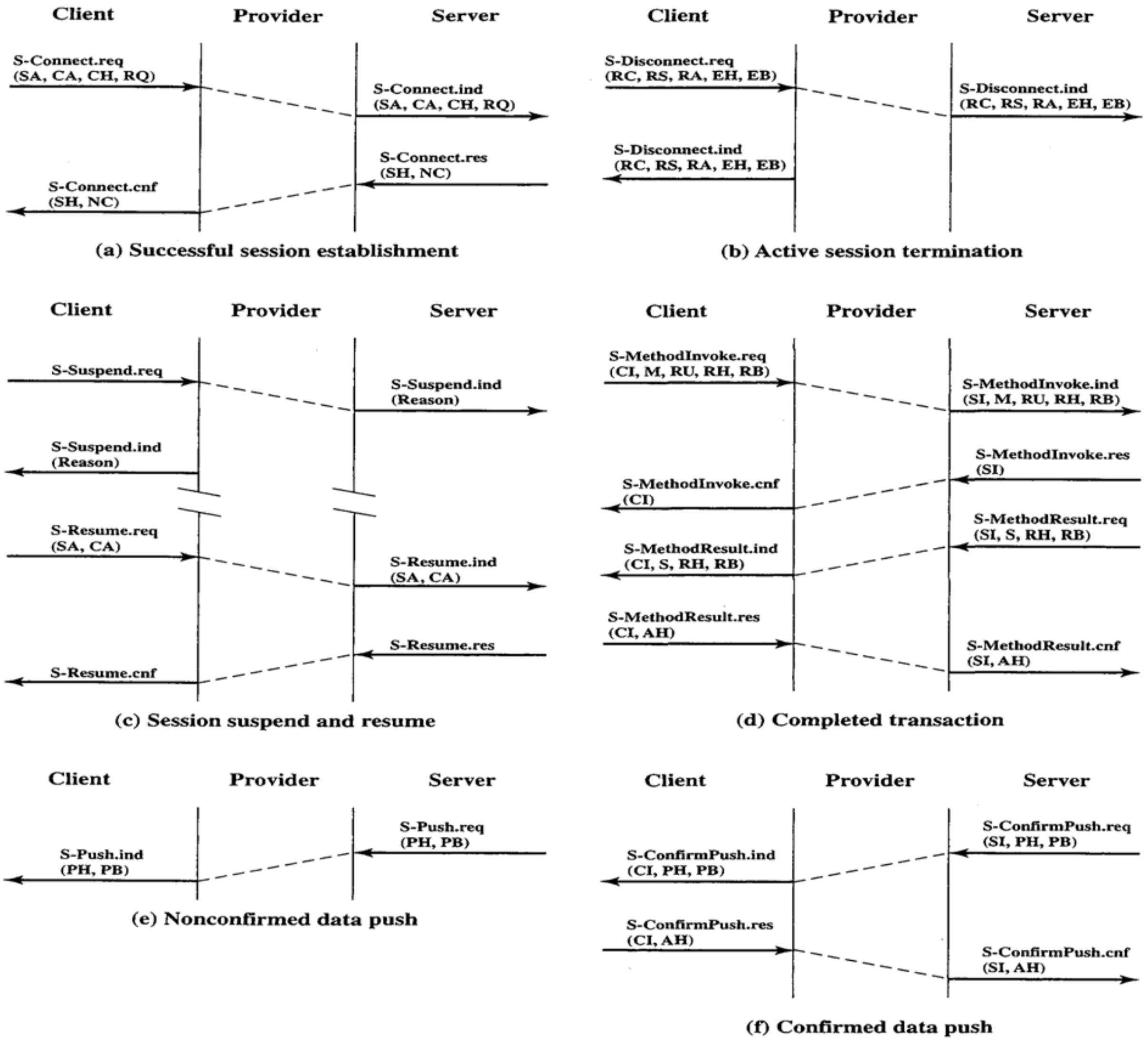
WSP is a transaction-oriented protocol based on the concept of a request and a reply. Each WSP protocol data unit (PDU) consists of a body, which may contain WML, WML Script, or images, and a header, which contains information about the data in the body and about the transaction.

WSP also defines a server Push operation, in which the server sends unrequested content to a client device. This may be used for broadcast messages or for services, such as news headlines or stock quotes, that may be tailored to each client device.

WSP Service In general, a connection-mode WSP provides the following services:

- Establish a reliable session from client to server and release that session in an orderly manner.
- Agree on a common level of protocol functionality using capability negotiation.
- Exchange content between client and server using compact encoding.
- Suspend and resume a session.
- Push content from server to client in an unsynchronized manner.

At the service level, WSP is defined in terms of a collection of service primitives, with associated parameters. These service primitives define the interface between WSP and users of WSP in the WAE.1 At the protocol level, the WSP specification defines a PDU format used to exchange data between peer WSP entities.


Client
Provider
Server
S-Connect.req (SA, CA, CH, RQ)
S-Connect.ind (SA, CA, CH, RQ)
S-Connect.res (SH, NC)
S-Connect.cnf (SH, NC)
Client
Provider
Server
S-Disconnect.req (RC, RS, RA, EH, EB)
S-Disconnect.ind (RC, RS, RA, EH, EB)
S-Disconnect.ind (RC, RS, RA, EH, EB)
Client
Provider
Server
S-Suspend.req
S-Suspend.ind (Reason)
S-Suspend.ind (Reason)
S-Resume.req (SA, CA)
S-Resume.ind (SA, CA)
S-Resume.res
S-Resume.cnf
Client
Provider
Server
S-MethodInvoke.req (CI, M, RU, RH, RB)
S-MethodInvoke.ind (SI, M, RU, RH, RB)
S-MethodInvoke.res (SI)
S-MethodInvoke.cnf (CI)
S-MethodResult.req (SI, S, RH, RB)
S-MethodResult.ind (CI, S, RH, RB)
S-MethodResult.res (CI, AH)
S-MethodResult.cnf (SI, AH)
Client
Provider
Server
S-Push.req (PH, PB)
S-Push.ind (PH, PB)
Client
Provider
Server
S-ConfirmPush.req (SI, PH, PB)
S-ConfirmPush.ind (CI, PH, PB)
S-ConfirmPush.res (CI, AH)
S-ConfirmPush.cnf (SI, AH)

(a) Successful session establishment

(b) Active session termination

(c) Session suspend and resume

(d) Completed transaction

(e) Nonconfirmed data push

(f) Confirmed data push

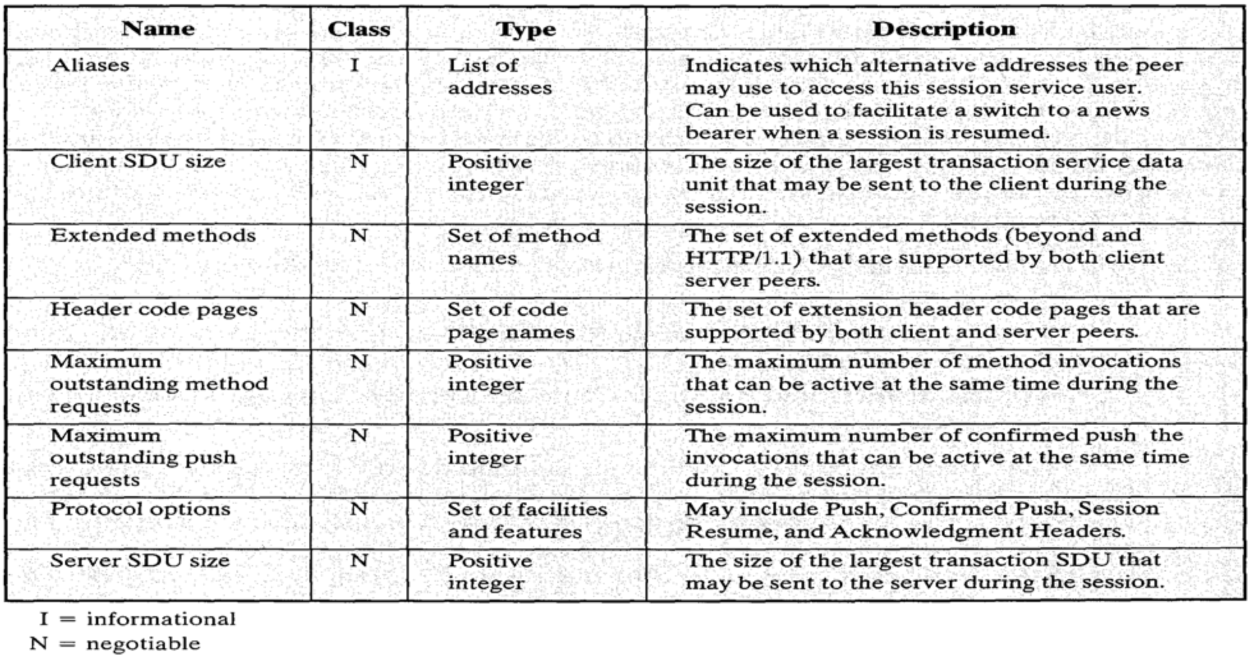
Figure 2. Wireless Session Protocol Primitives and Parameters

Above figure shows the key WSP transaction types in terms of the primitives and parameters that are exchanged.

Session establishment involves the exchange of S-Connect primitives (Figure 2). A WSP user acting as a client (mobile node side of the transaction) requests a session with a WSP user acting as a server (Web Server) on a remote system by issuing an S-Connect.req to WSP. Four parameters accompany the request:

- Server address: The peer with which the session is to be established.
- Client address: The originator of the session.
- Client headers: Contain attribute information that can be used for application level parameters to be communicated to the peer. This information is passed without modification by WSP and is not processed by WSP.
- **Requested capabilities:** A set of capabilities for this session requested by the client; these are listed in Table below. The client's WSP then prepares a WSP PDU, containing these parameters, to convey the request to the peer WSP at the server. The server address, client address, and client headers are unchanged. However, the WSP service provider at the client or the WSP service provider at the server, or both, may modify the set of requested capabilities so that they do not imply a higher level of functionality than the provider can support. With this possible modification, an S-Connect.ind containing the same parameters as in the request is delivered to the WSP user at the server side. If the WSP user at the server accepts the session request, it responds by invoking WSP with an S-Connect.rsp containing server headers and negotiated capabilities. The negotiated

Wireless Session Protocol Capabilities



Name	Class	Type	Description
Aliases	I	List of addresses	Indicates which alternative addresses the peer may use to access this session service user. Can be used to facilitate a switch to a news bearer when a session is resumed.
Client SDU size	N	Positive integer	The size of the largest transaction service data unit that may be sent to the client during the session.
Extended methods	N	Set of method names	The set of extended methods (beyond and HTTP/1.1) that are supported by both client server peers.
Header code pages	N	Set of code page names	The set of extension header code pages that are supported by both client and server peers.
Maximum outstanding method requests	N	Positive integer	The maximum number of method invocations that can be active at the same time during the session.
Maximum outstanding push requests	N	Positive integer	The maximum number of confirmed push the invocations that can be active at the same time during the session.
Protocol options	N	Set of facilities and features	May include Push, Confirmed Push, Session Resume, and Acknowledgment Headers.
Server SDU size	N	Positive integer	The size of the largest transaction SDU that may be sent to the server during the session.

I = informational
N = negotiable

Capabilities parameter is optional. If it is absent, the WSP user agrees to the set of capabilities proposed in the S-Connect.ind. If it is present, it reflects the level of functionality that the WSP user will accept. Finally, an S-Connect.ind is delivered to the original requester, containing the server headers and the final set of negotiated capabilities. The S-Disconnect primitive is used for **session termination.** Figure 2.b shows the case in which the client WSP user initiates the termination.

The request primitive includes the following parameters:

• **Reason code:** Cause of disconnection. If the cause is that the client is being redirected to contact a new server address, the next two parameters must be present.

• **Redirect security:** Indicates whether or not the client may reuse the current secure session when redirecting.

• **Redirect addresses:** Alternate addresses to be used to establish a session.

• **Error headers and error body:** If the termination is due to an error, these parameters may be included to provide information to the server WSP user about the error.

WSP acknowledges the receipt of the request by returning an S-Disconnect.ind to the client WSP user and conveying an S-Disconnect.ind to the server WSP user.

WSP supports **session suspend and resume.** An example of the use of this feature is when the client knows that it may be temporarily unavailable, due to roaming or disconnect and reconnect of the client device to the network. When a session is suspended, the state of the session is saved on both the client and server side and any in-transit data are lost. Figure 2.c shows the sequence involved when the suspend and resume are initiated by the client. For suspension, the only parameter is a reason code in the S-Suspend.ind primitive. When a resume request is issued, the server address and client address are present in the request and indication primitives.

A **transaction** involves an exchange of data between a client and server using the S-MethodInvoke and S-MethodResult primitives (Figure 2.d). S-MethodInvoke is used to request an operation to be executed by the server.

The request contains the following parameters:

• **Client Transaction ID:** Used to distinguish between pending transactions

• **Method:** Identifies the requested operation

• **Request URI (uniform resource identifier):** Specifies the entity to which the operation applies

• **Request headers and body:** Attribute information and data associated with the request

The indication conveyed to the server includes the same parameters except that the client transaction **ID** is replaced by a server transaction ID. The response and confirm primitives are used to confirm that the request has been conveyed and contain transaction IDs.

S-Method Result is used to return a response to an operation request. The request issued by the server includes the server transaction ID, the status associated with this response, and response headers and body containing attribute information and data associated with the response. The response and confirm primitives are used to confirm that the request has been conveyed and contain transaction IDs. These two primitives may also contain acknowledgment headers used to return some information to the server.

The non confirmed data push is used to send unsolicited information from the server to the client (Figure 2.e).The only parameters associated with these primitives are push headers and a push body containing attributes and the information to be conveyed. With confirmed data push, the server receives a confirmation that the push data have been delivered to the client. In addition to push headers and a push body, the confirmed data push primitives include a push ID; the respond and confirm primitives may also include acknowledgment headers.
The connectionless session service provides a non-confirmed capability for exchanging content entities between WSP users. Only the method invocation and push facilities are available. WSP Protocol Data Units WSP conveys service requests and responses in WSP PDUs. Each PDU is passed down to the transport layer to be included as the body of a transport-level PDU At the top level, the WSP PDU consists of three fields. The TID field is used to associated requests with replies in the connectionless WSP service and is not present in the connection-mode service. The Type field specifies the type and function of the PDU and basically corresponds to the type of service primitive that invoked WSP. Finally, the Type-Specific Contents contain all of the information to be conveyed as a result of a WSP service primitive.

Wireless Transaction Protocol

WTP manages transactions by conveying requests and responses between a user agent (such as a WAP browser) and an application server for such activities as browsing and e-commerce transactions. WTP provides a reliable transport service but dispenses with much of the overhead of TCP, resulting in a lightweight protocol that is suitable for implementation in "thin" clients (e.g., mobile nodes) and suitable for use over low-bandwidth wireless links.
WTP includes the following features:

- Three classes of transaction service.
- Optional user-to-user reliability: WTP user triggers the confirmation of each received message.
- Optional out-of-band data on acknowledgments.
- PDU concatenation and delayed acknowledgment to reduce the number of messages sent.
- Asynchronous transactions.

WTP is transaction oriented rather than connection oriented. With WTP, there is no explicit connection setup or teardown but rather a reliable connectionless service.

WTP Transaction Classes WTP provides three transaction classes that may be invoked by WSP or another higher layer protocol:

- Class 0: Unreliable invoke message with no result message
- Class 1: Reliable invoke message with no result message
- Class 2: Unreliable invoke message with one reliable result message

- Class 0 provides an unreliable datagram service, which can be used for an unreliable push operation. Data from a WTP user are encapsulated by WTP (the initiator, or client) in an

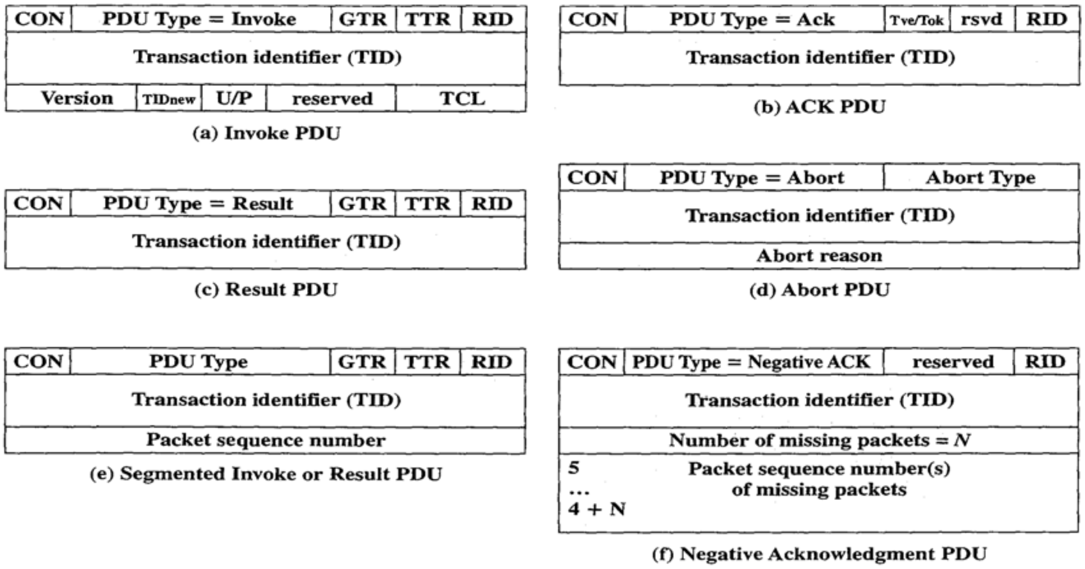
Invoke PDU and transmitted to the target WTP (the responder, or server), with no acknowledgment. The responder WTP delivers the data to the target WTP user.

- Class 1 provides a reliable datagram service, which can be used for a reliable push operation. Data from an initiator are encapsulated in an Invoke PDU and transmitted to the responder. The responder delivers the data to the target WTP user and acknowledges receipt of the data by sending back an ACK PDU to the WTP entity on the initiator side, which confirms the transaction to the source WTP user. The responder WTP maintains state information for some time after the ACK has been sent to handle possible retransmission of the ACK if it gets lost and/or the initiator retransmits the Invoke PDU.
- Class 2 provides a request/response transaction service and supports the execution of multiple transactions during one WSP session. Data from an initiator are encapsulated in an Invoke PDU and transmitted to the responder, which delivers the data to the target WTP user. The target WTP user prepares response data, which are handed down to the local WTP entity. The responder WTP entity sends these data back in a result PDU If there is a delay in generating the response data beyond a timer threshold, the responder may send an ACK PDU before sending the result PDU This prevents the initiator from unnecessarily retransmitting the Invoke message.

Protocol Format and Operation WTP makes use of six types of PDUs. Each PDU begins with a fixed header portion (Figure 3) and may be followed by a variable header portion that contains supplementary control information. The supplementary information is in the form of one or more transaction protocol items (TPIs).

The Invoke PDU is used to convey a request from an initiator to a responder; it is four bytes long and includes the following fixed header fields:

- Continue Flag: If this flag is set, there are one or more TPIs following the fixed header. In turn, each TPI begins with a continue flag bit to indicate whether there are more TPIs to follow or this is the last TPI.
- PDU Type: Indicates that this is an Invoke PDU
- Group Trailer Flag: Used when segmentation and reassembly are employed, as explained subsequently.
- Transmission Trailer Flag: Also used with segmentation and reassembly.
- Retransmission Indicator: Indicates whether this is a retransmission. The initiator will retransmit an Invoke PDU if it does not receive an acknowledgment within a specified time.
- Transaction Identifier: Used to associate a PDU with a particular transaction.
- Version: Version of WTP.
- TID new Flag: Set when the initiator has "wrapped" the TID value; that is, the next TID will be lower than the previous one.
- UIP Flag: When set, it indicates that the initiator require a user acknowledgment from the server WTP user. This means the WTP user confirms every received message. When this flag is clear, the responding WTP entity may acknowledge an incoming PDU without a confirmation from its user.
- Transaction Class: Indicates the desired transaction class to be used in processing this Invoke PDU


CON
PDU Type = Invoke
GTR
TTR
RID
Transaction identifier (TID)
Version
TIDnew
U/P
reserved
TCL
(a) Invoke PDU
CON
PDU Type = Ack
Tve/Tok
rsvd
RID
Transaction identifier (TID)
(b) ACK PDU
CON
PDU Type = Result
GTR
TTR
RID
Transaction identifier (TID)
(c) Result PDU
CON
PDU Type = Abort
Abort Type
Transaction identifier (TID)
Abort reason
(d) Abort PDU
CON
PDU Type
GTR
TTR
RID
Transaction identifier (TID)
Packet sequence number
(e) Segmented Invoke or Result PDU
CON
PDU Type = Negative ACK
reserved
RID
Transaction identifier (TID)
Number of missing packets = N
5
...
4 + N
Packet sequence number(s) of missing packets
(f) Negative Acknowledgment PDU

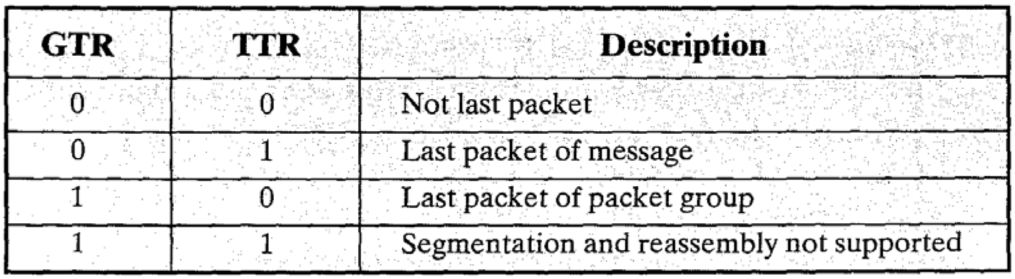
CON = continue flag
GTR = group trailer
TTR = transmission trailer
RID = retransmission indicator

TIDnew = TIDnew flag
U/P = user/provider acknowledgment flag
TCL = transaction class
Tve/Tok = TID verify/TID OK flag

Figure: WTP PDU Fixed Header Formats

If the message to be sent by WTP (the block of data from WSP) is too large for the current bearer, WTP may segment that message and send it in multiple packets, one per Invoke PDU When a message is sent in a large number of small packets; the packets may be sent and acknowledged in groups. Table 12.6 shows how the GTR and TTR flags are used to manage the process.

Table Group Trailer (GTR) and Transmission Trailer (TTR) Combinations



GTR	TTR	Description
0	0	Not last packet
0	1	Last packet of message
1	0	Last packet of packet group
1	1	Segmentation and reassembly not supported

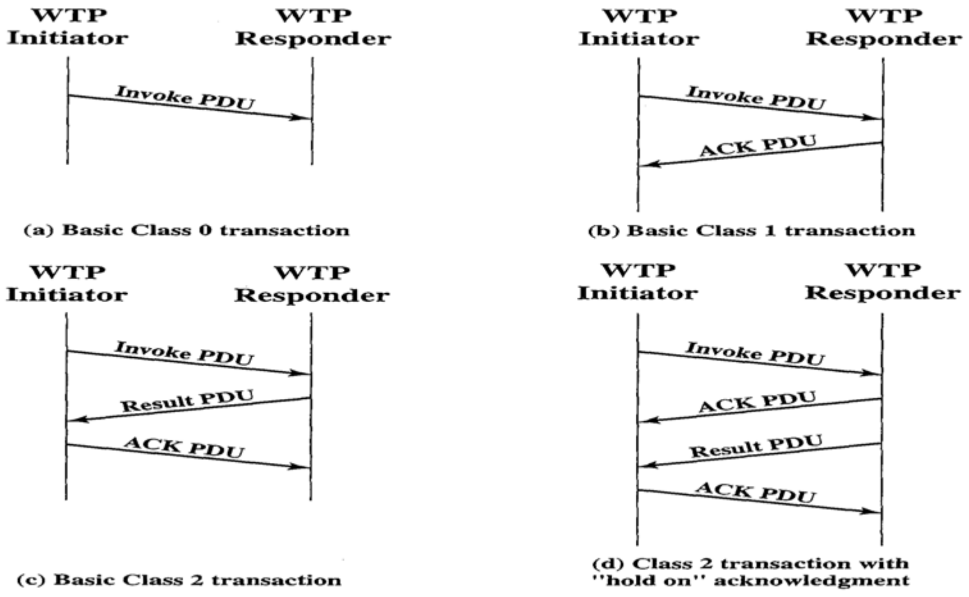
The ACK PDU is used to acknowledge an Invoke or Result PDU It is three bytes long. The PDU includes a Tve/Tok flag, whose interpretation depends on the direction of the PDU In the direction from the responder to the initiator, this is a Tve flag. If the Tve flag is set, it has the interpretation, "Do you have an outstanding transaction with this TID?" In the other direction, if the Tok flag is set, it means, "I have an outstanding transaction with this TID."

The Result PDU is a 3-byte PDU used to convey the response of the server to the client.

The Abort PDU is used to abort a transaction. Two abort types are defined: user and provider. If the abort is generated by the WTP user (e.g., WSP), then the user's reason for the abort is conveyed in the body of the PDU and provided to the WTP user at the destination of the abort PDU If the abort is generated by the WTP provider (the WTP entity that is sending this abort PDU), then the abort reason field in the PDU indicates one of the following reasons:

- Unknown: Unexplained error.
- Protocol error: The received PDU could not be interpreted.
- Invalid TID: Used by the initiator as a negative result to the TID verification.
- Not implemented Class 2: The respondent does not support class 2, which was requested.
- Not implemented SAR: The respondent does not support segmentation and reassembly.
- Not implemented user acknowledgment: The responder does not support user acknowledgment.
- WTP version 1: The initiator requested a version of WTP that is not supported; current version is l.
- Capacity temporarily exceeded: Due to an overload situation, transaction cannot be completed.

The segmented invoke PDU and the segmented result PDU may be used for segmentation and reassembly. When they are used, each packet is numbered sequentially. The negative acknowledgment PDU is used to indicate that one or more packets in a sequence did not arrive.
Figure shows some basic examples of the time sequence of the use of WTP PDUs for the three classes of operation.
WTP Service: The WTP service is defined by three primitives. TR-Invoke is used to initiate a new transaction. TR-Result is used to send back a result of a previously initiated transaction. And Tr-Abort is used to abort an existing transaction.



(a) Basic Class 0 transaction

(b) Basic Class 1 transaction

(c) Basic Class 2 transaction

(d) Class 2 transaction with "hold on" acknowledgment

Figure: Examples of WTP Operation

Q 51) What functions are supported by WML? In brief, describe WTLS security services.

Ans:

Wireless Markup Language
WML was designed to describe content and format for presenting data on devices with limited bandwidth, limited screen size, and limited user input capability. It is designed to work with telephone keypads, styluses, and other input devices common to mobile, wireless communication. WML permits the scaling of displays for use on two-line screens found in some small devices, as well as the larger screens found on smart phones.

.

For an ordinary PC, a Web browser provides content in the form of Web pages coded with the Hypertext Markup Language (HTML). To translate an HTML coded Web page into WML with content and format suitable for wireless devices, much of the information, especially graphics and animation, must be stripped away. WML presents mainly text-based information that attempts to capture the essence of the Web page and that is organized for easy access for users of mobile devices.

Important features of WML include the following:
• Text and image support: Formatting and layout commands are provided for text and limited image capability.
• Deck/card organizational metaphor: WML documents are subdivided into small, well-defined units of user interaction called cards. Users navigate by moving back and forth between cards. A card specifies one or more units of interaction (a menu, a screen of text, or a text-entry field). A WML deck is similar to an HTML page in that it is identified by a Web address (URL) and is the unit of content transmission.
• Support for navigation among cards and decks: WML includes provisions for event handling, which is used for navigation or executing scripts.

Wireless Transport Layer Security:
WTLS provides security services between the mobile device (client) and the WAP gateway. WTLS is based on the industry-standard Transport Layer Security (TLS) Protocol, which is a refinement of the secure sockets layer (SSL). TLS is the standard security protocol used between Web browsers and Web servers.2 WTLS is more efficient that TLS, requiring fewer message exchanges. To provide end-to-end security, WTLS is used between the client and the gateway, and TLS is used between the gateway and the target server. WAP systems translate between WTLS and TLS within the WAP gateway. Thus, the gateway is a point of vulnerability and must be given a high level of security from external attacks.

WTLS provides the following features:

- Data integrity: Ensures that data sent between the client and the gateway are not modified, using message authentication
- Privacy: Ensures that the data cannot be read by a third party, using encryption
- Authentication: Establishes the authentication of the two parties, using digital certificates

- Denial-of-service protection: Detects and rejects messages that are replayed or not successfully verified

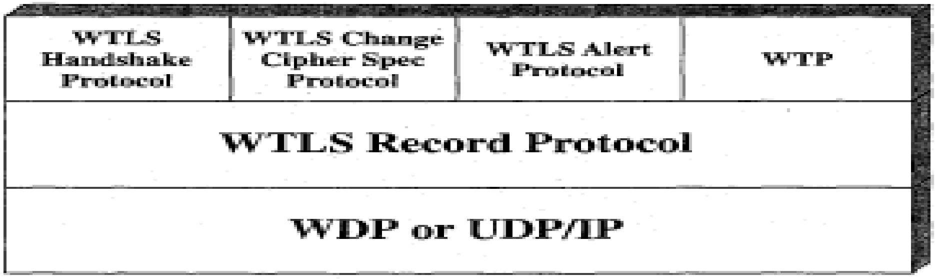


Figure 12.16 WTLS Protocol Stack

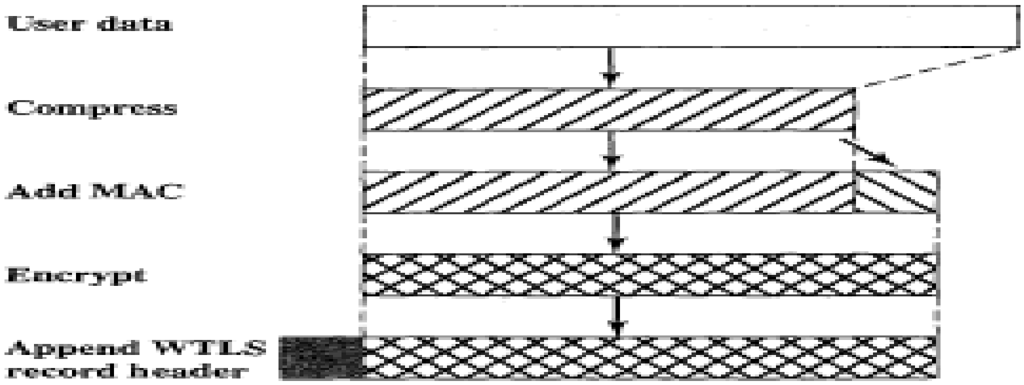


Figure 12.17 WTLS Record Protocol Operation

Q 52) Write Short Notes on:

a. Antenna

An antenna (or aerial) is a transducer that transmits or receives electromagnetic waves. In other words, antennas convert electromagnetic radiation into electrical current, or vice versa. Antennas generally deal in the transmission and reception of radio waves, and are a necessary part of all radio equipment.

Antennas are used in systems such as radio and television broadcasting, point-to-point radio communication, wireless LAN, cell phones, radar, and spacecraft communication. Antennas are most commonly employed in air or outer space, but can also be operated under water or even through soil and rock at certain frequencies for short distances.

Basic antenna models

(i) The Isotropic radiator is a purely theoretical antenna that radiates equally in all directions. It is considered to be a point in space with no dimensions and no mass. This antenna cannot physically exist, but is useful as a theoretical model for comparison with all other antennas. Most antennas' gains are measured with reference to an isotropic radiator, and are rated in dBi (decibels with respect to an isotropic radiator).

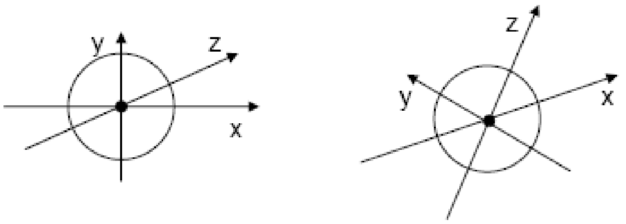


Fig: Radiation pattern

(ii) The dipole antenna is simply two wires pointed in opposite directions arranged either horizontally or vertically, with one end of each wire connected to the radio and the other end hanging free in space. Since this is the simplest practical antenna, it is also used as a reference model for other antennas; gain with respect to a dipole is labeled as dBd.

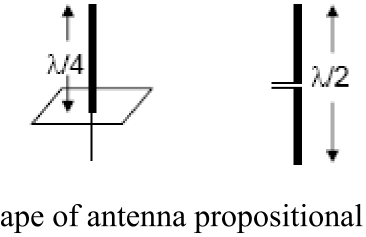


Fig: Shape of antenna propositional to wavelength

Generally, the dipole is considered to be omnidirectional in the plane perpendicular to the axis of the antenna, but it has deep nulls in the directions of the axis. Variations of the dipole include the folded dipole, the half wave antenna, the ground plane antenna, the whip, and the J-pole.

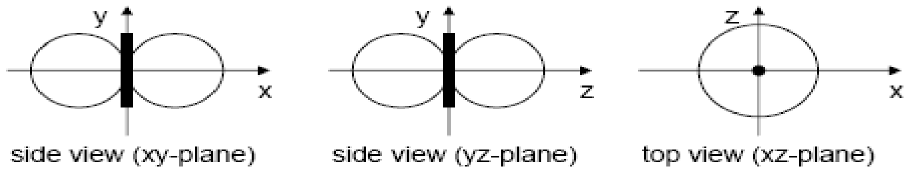


Fig: Radiation Pattern of dipole antenna

(iii) A directional antenna or beam antenna is an antenna which radiates greater power in one or more directions allowing for increased performance on transmit and receive and reduced interference from unwanted sources. Directional antennas like yagi antennas provide increased performance over dipole antennas when a greater concentration of radiation in a certain direction is desired.

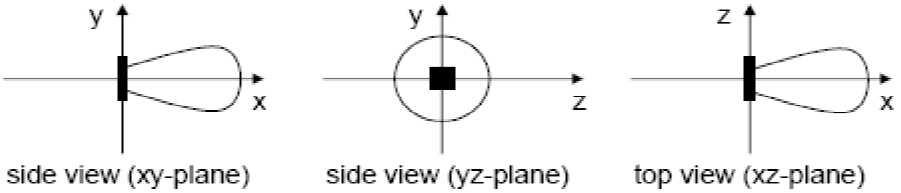


Fig: Radiation Pattern of directional antenna

(iv) A sector antenna is a kind of directional antenna with a sector-shaped radiation pattern. In mobile communications, these antennas are typically installed in base-station sites for point-to-multipoint connections used in mobile communications. The coverage area which is equal to the square of sector's projection to the ground can be adjusted by changing electrical or mechanical down tilts

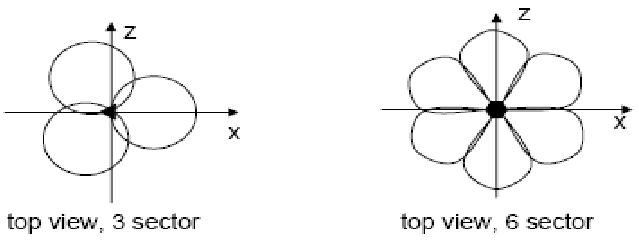


Fig: Radiation Pattern of sector antenna

(v) Diversity Antenna, also known as space diversity, is any one of several wireless diversity schemes that use two or more antennas to improve the quality and reliability of a wireless link. Often, especially in urban and indoor environments, there is not a clear line-of-sight (LOS) between transmitter and receiver. Instead the signal is reflected along multiple paths before finally being received. Each of these bounces can introduce phase shifts, time delays, attenuations, and even distortions that can destructively interfere with one another at the aperture of the receiving antenna.

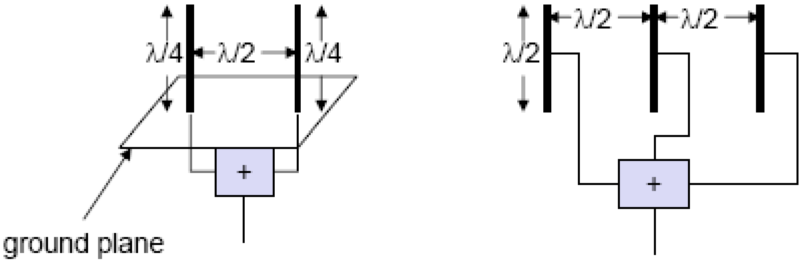


Fig: Diversity antenna systems

Diversity combining constitutes a combination of the power of all signals to produce gain. The phase is first corrected (cophasing) to avoid cancellation. As shown in the fig., different schemes are possible. On the left, two λ/4 antennas are combined with a distance of λ/2 between them on top of a ground plane. On the right, three standard λ/2 dipoles are combined with a distance of λ/2 between them. Spacing could also be in multiples of λ/2.

b. Symbian OS

Symbian OS is one of Nokia's mobile operating systems for mobile devices and low-end smartphones, with associated libraries, user interface, frameworks and reference implementations of common tools, originally developed by Symbian Ltd. The Symbian Operating System is an operating system designed mainly for mobile devices.

Symbian OS 9.5 version is the latest version to have been released by the Symbian Operating System. It delivers more than seventy new features for high-performance. It is one of the most powerful smart phones at affordable market costs and an easy operating system with a friendly interface for everyone to use whether he is in Europe, America or in parts of Asia.

It is designed for the specific requirements of advanced 2.5Generation and 3Generation mobile phones. Symbian Operating System also provides numerous applications which can be used by the Customers like alarm Clocks, Calendars, Business tools, games, themes and numerous other applications.

Structure

The Symbian System Model contains the following layers, from top to bottom:

- UI Framework Layer
- Application Services Layer
    1. Java ME
- OS Services Layer
    1. generic OS services
    2. communications services
    3. multimedia and graphics services
    4. connectivity services
- Base Services Layer
- Kernel Services & Hardware Interface Layer

The Base Services Layer is the lowest level reachable by user-side operations; it includes the File Server and User Library, a Plug-InFramework which manages all plug-ins, Store, Central Repository, DBMS and cryptographic services. It also includes the Text Window Server and the Text Shell: the two basic services from which a completely functional port can be created without the need for any higher layer services.

Symbian has a microkernel architecture, which means that the minimum necessary is within the kernel to maximise robustness, availability and responsiveness. It contains a scheduler, memory management and device drivers, but other services like networking, telephony andfilesystem support are placed in the OS Services Layer or the Base Services Layer. The inclusion of device drivers means the kernel is not a*true* microkernel. The EKA2 real-time kernel, which has been termed a nanokernel, contains only the most basic primitives and requires an extended kernel to implement any other abstractions.

Symbian is designed to emphasise compatibility with other devices, especially removable media file systems. Early development of EPOC led to adopting FAT as the internal file system, and this remains, but an object-oriented persistence model was placed over the underlying FAT to provide a POSIX-style interface and a streaming model. The internal data formats rely on using the same APIs that create the data to run all file manipulations. This has resulted in data-dependence and associated difficulties with changes and data migration.

There is a large networking and communication subsystem, which has three main servers called: ETEL (EPOC telephony), ESOCK (EPOC sockets) and C32 (responsible for serial communication). Each of these has a plug-in scheme. For example ESOCK allows different ".PRT" protocol modules to implement various networking protocol schemes. The subsystem also contains code that supports short-range communication links, such as Bluetooth, IrDA and USB.

There is also a large volume of user interface (UI) Code. Only the base classes and substructure were contained in Symbian OS, while most of the actual user interfaces were maintained by third parties. This is no longer the case. The three major UIs - S60, UIQ and MOAP - were contributed to Symbian in 2009. Symbian also contains graphics, text layout and font rendering libraries.

All native Symbian C++ applications are built up from three framework classes defined by the application architecture: an application class, a document class and an application user interface class. These classes create the fundamental application behaviour. The remaining required functions, the application view, data model and data interface, are created independently and interact solely through their APIs with the other classes.

Features Of Symbian Operating System

- Generally, the language C++ is used in most of the symbian operating systems. But in many Symbian Operating System the operating system can also use languages like Python, Visual Basic, OPL and Perl
- Symbian Operating System was built in such a way that it follows the three basic design rules. The integrity and security of user data is of paramount importance. Response time must not be as small as possible. All resources are scarce.
- Symbian OS programming is said to be event-based, and the Central Processing Unit is switched off when the running applications and programs are not linked to the event. This is achieved through a programming logic called active objects.
- The Symbian Operating system is compatible with all kinds of devices, mostly removable media file systems.
- Symbian Operating system 9.x which is one of the latest models has adopted a better model.
- The Symbian system is not an Open Source software. Cell phone manufacturers, though have some parts of its source code.
- The Symbian applications like the Themes, games, wall papers and softwares are all SIS files which can also be easily transferred by using Bluetooth, or through the internet or through transfer using cables.

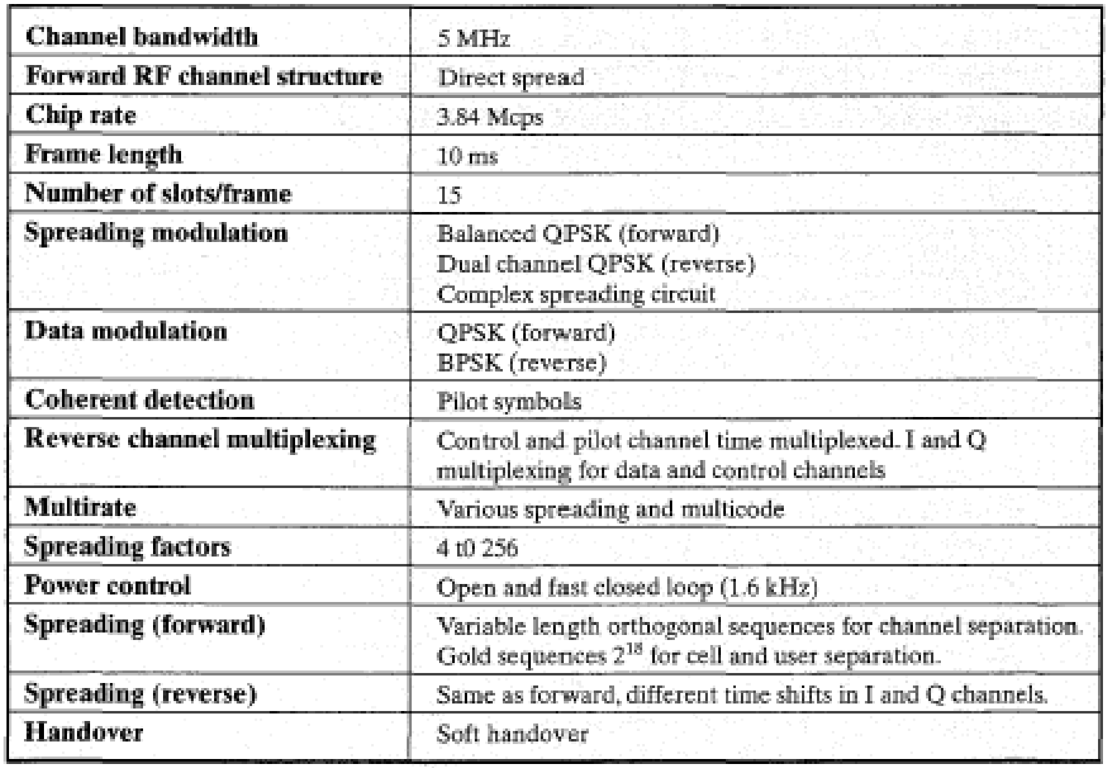
e. WCDMA

WCDMA (Wideband Code Division Multiple Access) is the radio access scheme used for third generation cellular systems that are being rolled out in various parts of the globe. The 3G systems to support wideband services like high-speed Internet access, video and high quality image transmission with the same quality as the fixed networks. The WCDMA standard was evolved through the Third Generation Partnership Project (3GPP) which aims to ensure interoperability between different 3G networks.

Key Features of WCDMA :

- Support high data rate transmission : 384 kbps with wide area coverage, 2Mbps with local coverage.
- High Service Flexibility : support of multiple parallel variable rate services on each connection.
- Both Frequency Division Duplex (FDD) and Time Division Duplex (TDD).
- Built in support for future capacity and coverage enhancing technologies like adaptive antennas, advanced receiver structures and transmitter diversity.
- Support of inter frequency hand over and hand over to other systems, including handover to GSM.
- Efficient packet access.

Table 10.8 W-CDMA Parameters



Channel bandwidth	5 MHz
Forward RF channel structure	Direct spread
Chip rate	3.84 Mcps
Frame length	10 ms
Number of slots/frame	15
Spreading modulation	Balanced QPSK (forward) Dual channel QPSK (reverse) Complex spreading circuit
Data modulation	QPSK (forward) BPSK (reverse)
Coherent detection	Pilot symbols
Reverse channel multiplexing	Control and pilot channel time multiplexed. I and Q multiplexing for data and control channels
Multirate	Various spreading and multicode
Spreading factors	4 t0 256
Power control	Open and fast closed loop (1.6 kHz)
Spreading (forward)	Variable length orthogonal sequences for channel separation. Gold sequences 2^{18} for cell and user separation.
Spreading (reverse)	Same as forward, different time shifts in I and Q channels.
Handover	Soft handover

g. MIDP:

The Mobile Information Device Profile (MIDP) is key element of the Java 2 Platform, Mobile Edition (J2ME). When combined with the Connected Limited Device Configuration (CLDC), MIDP provides a standard runtime Java environment for today's most popular mobile information devices, such as cell phones and mainstream personal digital assistants (PDAs). The MIDP specification was defined through the Java Community Process (JCP) by an expert group of more than 50 companies, including leading device manufacturers, wireless carriers, and vendors of mobile software. It defines a platform for dynamically and securely deploying, optimized, graphical, networked applications.

Specifications

MIDP 2.0 (JSR 118) is a revised version of the MIDP 1.0 specification. New features include an enhanced user interface, multimedia and game functionality, more extensive connectivity, over-the air provisioning (OTA),and end to end security.

MIDP 1.0 (JSR 37) is the original specification, which provides core application functionality required by mobile applications, including basic user interface and network security.

Benefits

- Rich User Interface Capabilities: MIDP applications provide the foundation for highly graphical and intuitive applications.
- Extensive Connectivity: MIDP enables developers to exploit the native data network and messaging capabilities of mobile information devices.
- Multimedia and Game Functionality: MIDP is ideal for building portable games and multimedia applications.
- Over –the-Air-Provisioning: A Major benefit of MIDP is its capability to deploy and update applications dynamically and securely, over the air.
- End to End Security: MIDP Provides a robust security model that complies with open standards and protects the network, applications, and mobile information devices.

h. WAP:

WAP 1.x is an earlier version of the WAP standard. The most current version is WAP 2.0. The markup language defined in WAP 2.0 is XHTML MP (XHTML Mobile Profile). It is a subset of the XHTML used on the web. XHTML MP supports a mobile version of cascading style sheet called WCSS (WAP CSS). It is a subset of the CSS2 used on the web plus some WAP specific extensions.

Most of the new mobile phone released are WAP 2.0 enabled. As WAP 2.0 is backward compatible to WAP 1.x, WAP 2.0 enabled mobile devices can display both XHTML MP and WML documents.

WML 1.x is an earlier technology. However, that does not mean it is of no use, since a lot of wireless devices that only supports WML 1.x are still being used Besides some useful features of WML are not available in XHTML MP. For example, XHTML MP does not support events, variables and client-side scripting.

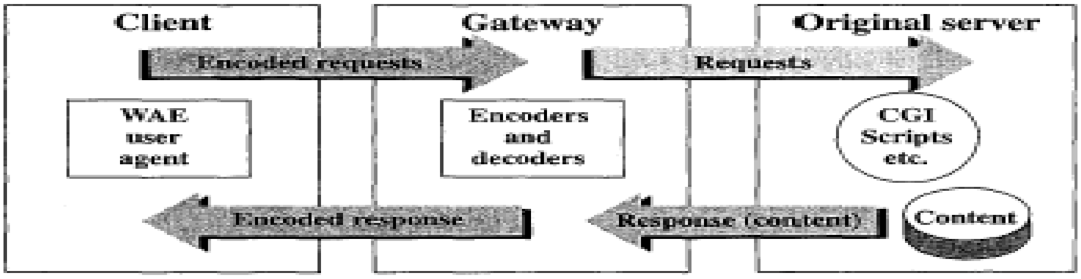
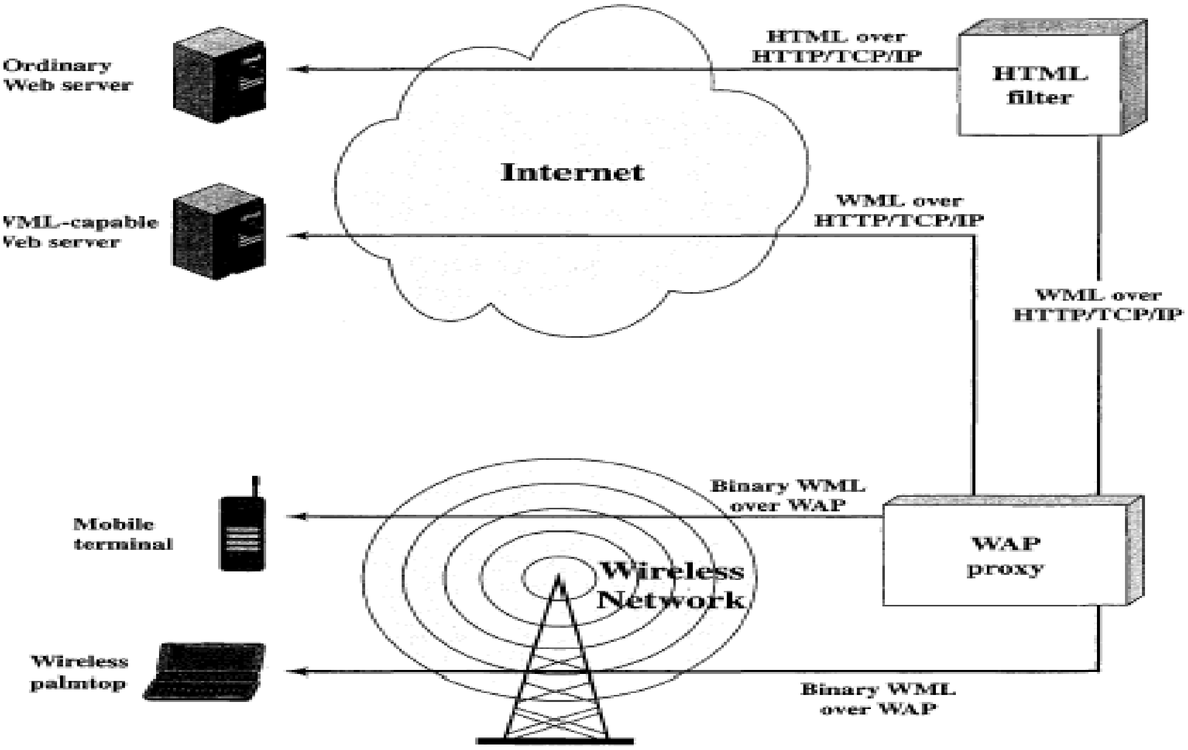


Figure 12.9 The WAP Programming Model



'igure 12.10 WAP Infrastructure

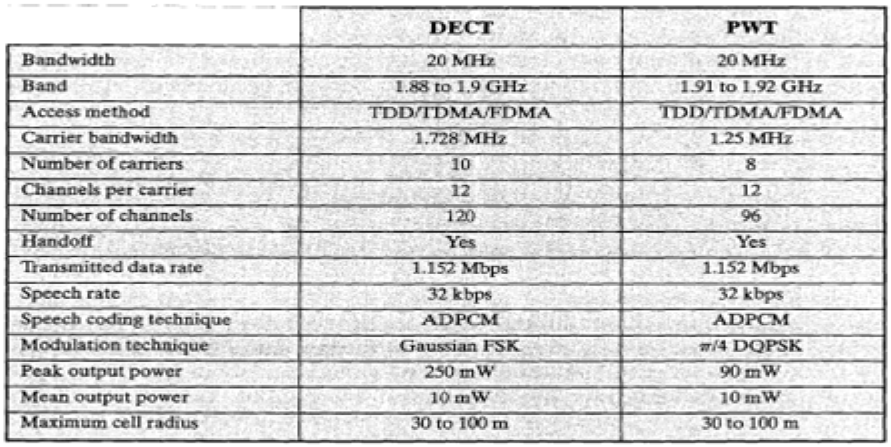
i. Cordless systems:

Standardized cordless systems have evolved from cordless telephone technology. Originally, cordless telephones were developed to provide users with mobility within a residence or small office by separating the handset from the rest of the telephone (called the base station) and providing a simple analog wireless link. technology improved, digital cordless telephones were developed. The products on the market used proprietary wireless interfaces. Because the same manufacturer sold the base station and the handset as a unit, there was no need for standards. Standards-making bodies became interested in standardizing cordless technology to widen its range of applicability, in two directions. First, cordless systems can support multiple users from the same base station, which could include either multiple telephone handsets or both voice and data devices (e.g., fax or printer). Second, cordless systems can operate in a number of environments:

- Residential: Within a residence a single base station can provide voice and data support, enabling in-house communications as well as providing a connection to the public telephone network.
- Office: A small office can be supported by a single base station that provides service for a number of telephone handsets and data devices. In a larger office, multiple base stations can be used in a cellular configuration, with the base stations connected to a PBX (private branch exchange) switch. Such a configuration can serve hundreds or even thousands of users.
- Telepoint: Telepoint refers to the provision of a base station in a public place, such as a shopping mall or airport. This application has not succeeded in the marketplace. A number of design considerations have driven the development of cordless standards.

Lists the following:

1. The range of the handset from the base station is modest, up to about 200 m. Thus, low-power designs are used. Typically, the power output is one or two orders of magnitude lower than for cellular systems.
2. The handset and the base station need to be inexpensive. This dictates the use of simple technical approaches, such as in the area of speech coding and channel equalization.
3. Frequency flexibility is limited, because the user owns the base station as well as the mobile portion and can install these in a variety of environments. Hence, the system needs to be able to seek a low-interference channel wherever it is used. Although a number of different standards have been proposed for cordless systems, the most prominent is DECT (digital enhanced cordless telecommunications)



	DECT	PWT
Bandwidth	20 MHz	20 MHz
Band	1.88 to 1.9 GHz	1.91 to 1.92 GHz
Access method	TDD/TDMA/FDMA	TDD/TDMA/FDMA
Carrier bandwidth	1.728 MHz	1.25 MHz
Number of carriers	10	8
Channels per carrier	12	12
Number of channels	120	96
Handoff	Yes	Yes
Transmitted data rate	1.152 Mbps	1.152 Mbps
Speech rate	32 kbps	32 kbps
Speech coding technique	ADPCM	ADPCM
Modulation technique	Gaussian FSK	π/4 DQPSK
Peak output power	250 mW	90 mW
Mean output power	10 mW	10 mW
Maximum cell radius	30 to 100 m	30 to 100 m

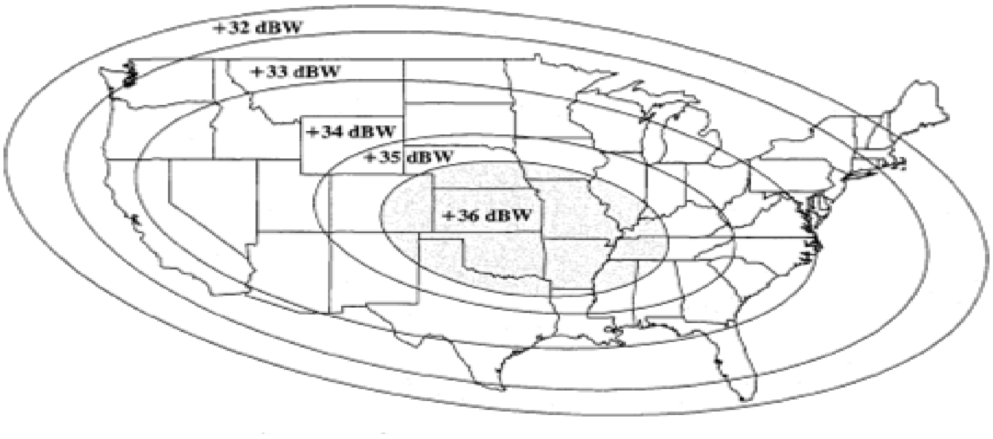
developed in Europe. The U.S. equivalent is known as PWT (personal wireless telecommunications). Table shows some of the key parameters for DECT and PWT. These systems use an approach referred to as time division duplex (TDD). We begin with a general discussion of TDD and then turn to the details of DECT.

j. Satellite Footprint

The footprint of a communications satellite is the ground area that its transponders offer coverage, and determines the satellite dish diameter required to receive each transponder's signal. There is usually a different map for each transponder (or group of transponders) as each may be aimed to cover different areas of the ground.

Footprint maps usually show either the estimated minimal satellite dish diameter required or the signal strength in each area measured in dBW.

At microwave frequencies, which are used in satellite communications, highly directional antennas are used. Thus, the signal from a satellite is not isotropically broadcast but is aimed at a specific point on the earth, depending on which area of coverage is desired. The center point of that area will receive the highest radiated power, and the power drops off as you move away from the center point in any direction. This effect is typically displayed in a pattern known as a satellite footprint; an example is shown in Figure. The satellite footprint displays the effective radiated power of the antenna at each point, taking into account the signal power fed into the antenna and the directionality of the antenna. In the example figure, the power for Arkansas is +36 dBW and for Massachusetts is +32 dBW. The actual power received at any point on the footprint is found by subtracting the free space loss from the effective power figure.



n. TDMA, DAMA, and SCPC access techniques in VSAT:

VSAT is an abbreviation for a Very Small Aperture Terminal. It is basically a two-way satellite ground station with less than 3 meters tall dish antenna stationed. The transmissions rates of VSATs are usually from very low and up to 4 Mbit/s . These VSATs primary job is accessing the satellites in the geosynchronous orbit and relaying data from terminals in earth to other terminals and hubs. They will often transmit narrowband data, such as the transactions of credit cards, polling, RFID (radio frequency identification) data , SCADA(Supervisory Control and Data Acquisition) , or broadband data, such as satellite Internet, VoIP, and videos. However, the VSAT technology is also used for various types of communications.

TDMA refers to Time Division Multiple Access offers a much more flexible scheme, which comprises all technologies that allocate certain time slots for communication. One basic scheme is demand assigned multiple access (DAMA) also called reservation Aloha, a scheme typical for satellite system. DAMA has two modes. During a connection phase following the slotted Aloha scheme , all stations can try to reserve future slots. For example different stations on earth try to reserve access time for satellite transmission. Collisions during the reservation phase do not destroy data transmission, but only the shorts request for data transmission.

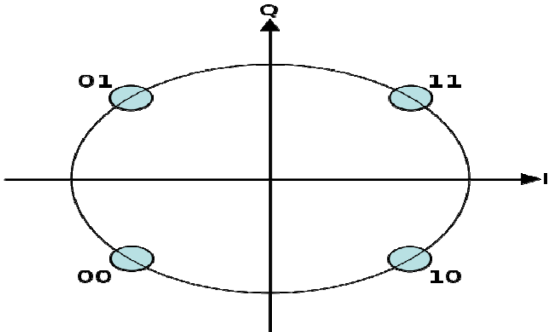
Equatorial Communications first used the spread spectrum technology also called as Single Channel Per Carrier (SCPC) technique .In this avoid groupings altogether and simply to divide the 36-MHz bandwidth into individual VF channels. SCPC is currently provided in the C band. A single 36-MHz channel is subdivided into 800 45-kHz analog channels, each dedicated to a simplex VF link, using FM. In 1985, the current world’s most used VSATs , the Ku band(12 to 14 GHz) was co-developed by Schlumberger Oilfield Research and Hughes Aerospace. It is primarily used to provide portable network connection for exploration units, particularly doing oil field drilling.

p. QPSK (Quadrature Phase Shift Keying)

Quadriphase PSK, 4-PSK, or 4-QAM. (Although the root concepts of QPSK and 4-QAM are different, the resulting modulated radio waves are exactly the same.) QPSK uses four points on the constellation diagram, equispaced around a circle. With four phases, QPSK can encode two bits per symbol, shown in the diagram with gray coding to minimize the bit error rate (BER) — sometimes misperceived as twice the BER of BPSK.

The mathematical analysis shows that QPSK can be used either to double the data rate compared with a BPSK system while maintaining the *same* bandwidth of the signal, or to *maintain the data-rate of BPSK* but halving the bandwidth needed. In this latter case, the BER of QPSK is *exactly the same* as the BER of BPSK - and deciding differently is a common confusion when considering or describing QPSK.

Given that radio communication channels are allocated by agencies such as the Federal Communication Commission giving a prescribed (maximum) bandwidth, the advantage of QPSK over BPSK becomes evident: QPSK transmits twice the data rate in a given bandwidth compared to BPSK - at the same BER. The engineering penalty that is paid is that QPSK transmitters and receivers are more complicated than the ones for BPSK. However, with modern electronics technology, the penalty in cost is very moderate.



Constellation diagram for QPSK with Gray coding. Each adjacent symbol only differs by one bit.

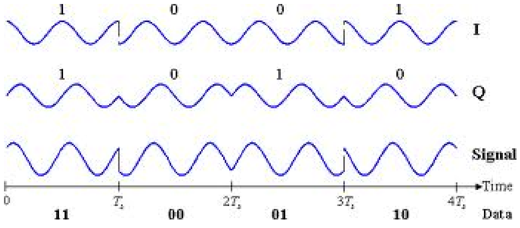


Fig: QPSK TIMING Diagram