May 2012

Q1 A) Discuss the architecture and the services provided by the IEEE 802.16?
Ans. **IEEE 802.16 Architecture:**
System Reference Architecture, The 802.16 standards are designed with respect to the abstract system reference model shown in figure below.

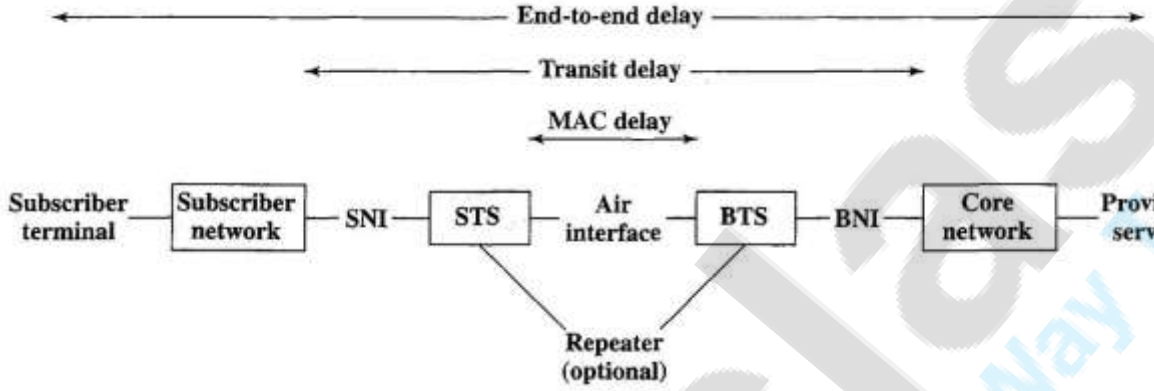


Figure 11.13 IEEE 802.16 System Reference Points

An 802.16 wireless service provides a communications path between a subscriber sites, 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). 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, as discussed subsequently in this subsection. The system reference model also shows interfaces between the transceiver stations and the networks behind them (SNI and BNI).The details of these interfaces are beyond the scope of the 802.16 standards. 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. Finally, the system reference model includes the optional use of some sort of repeater. The air interface specification allows for the possibility of repeaters or reflectors to bypass obstructions and extend cell coverage.

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) 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.

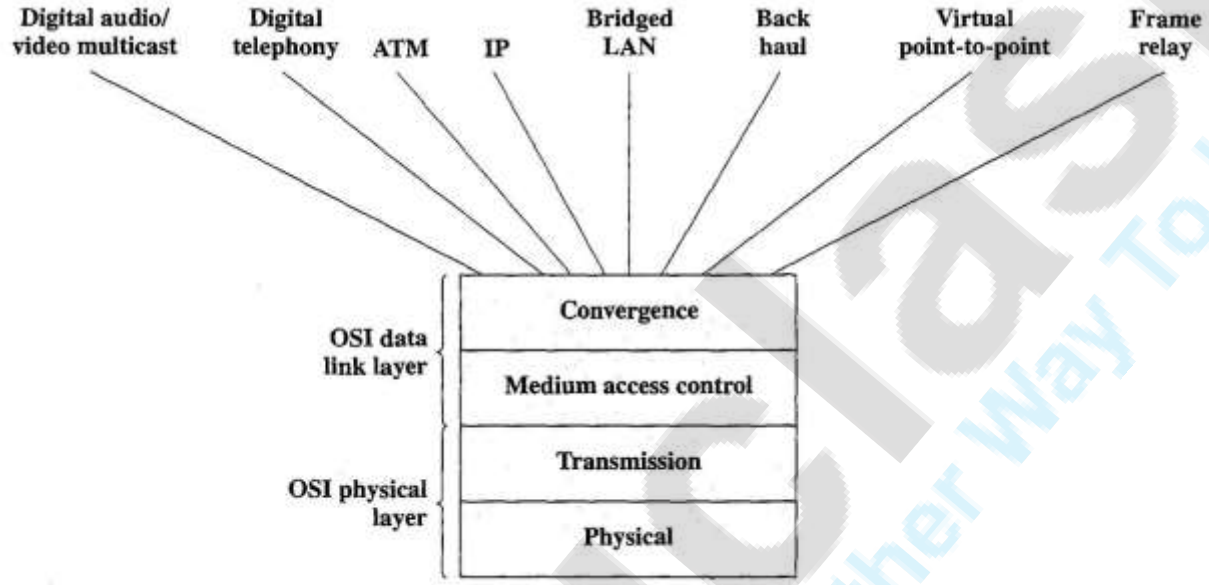


Figure 11.14 IEEE 802.16 Protocol Architecture

Figure 11.14 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

In addition, the physical layer of the 802 model includes a specification of the transmission medium and the frequency band. Generally, this is considered "below" the lowest layer of the OSI model. However, the choice of transmission medium and frequency band is critical in wireless link design, and so a specification of the medium is included. 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. In the downstream direction (base station to subscriber stations), there is only one transmitter and the MAC protocol is relatively simple. In the upstream direction, multiple subscriber stations are competing for access, resulting in a more complex MAC protocol.
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.

In some cases, such as digital audio and video, no convergence layer is needed and the stream of digital data is presented to the transmission layer. Upper-layer services that make use of a PDU structure do require a convergence layer.

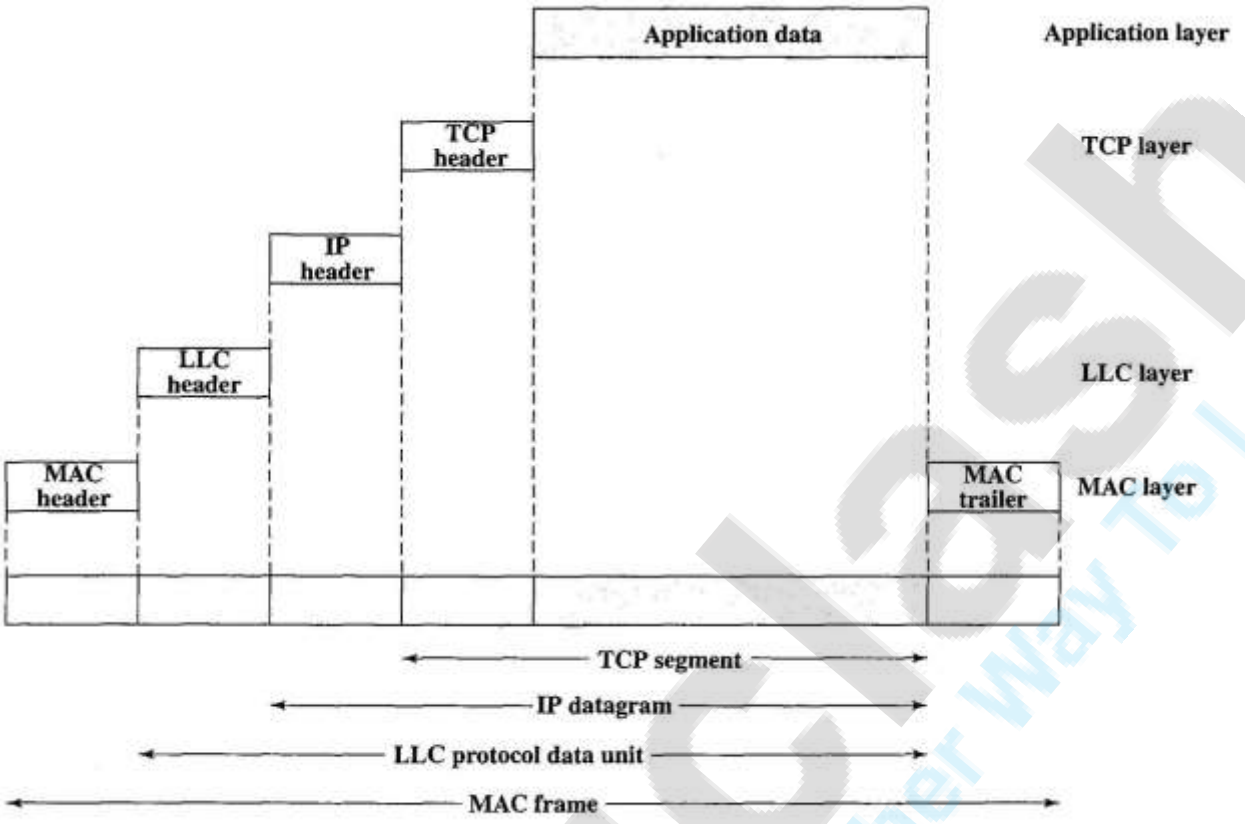


Figure 11.15 IEEE 802.16 Protocols in Context

An example of the protocol structure supported by the convergence layer is the handling of TCP/IP based traffic, as shown in Figure 11.15 (compare Figure 4.2). Higher-level data are passed down to LLC (logical link control), which appends control information as a header, creating an LLC protocol data unit (PDU). This control information is used in the operation of the LLC protocol, which is a form of data link control protocol (see Appendix C). The entire LLC PDU is then passed down to the MAC layer, which appends control information at the front and back of the packet, forming a MAC frame. Again, the control information in the frame is needed for the operation of the MAC protocol. The figure shows the use of TCP/IP and an application layer above the 802.16 protocols.

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. A special case of this service is two-way video such as in teleconferencing. In this latter case, delay requirements are stringent because of the interactivity involved.

• 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.

Another way of viewing the service requirements for 802.16 is shown in Table 11.10, which is taken from the 802.16 functional requirements document. 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.

Table 11.10 IEEE 802.16 Services and QoS Requirements

	Bearer Service	MAC Payload Rate	Maximum Ratio	Maximum Delay (one way)
Circuit Based	High-quality narrowband/ Voice frequency telephony (Vocoder MOS ≥ 4.0)	32 to 64 kbps	BER 10^{-6}	5 ms
	Lower quality narrowband/ Voice frequency telephony (Vocoder MOS < 4.0)	6 to 16 kbps	BER 10^{-4}	10 ms
	Trunking	≤155 Mbps	BER 10^{-6}	5 ms
Variable Packet	Time critical packet services	4 to 13 kbps (voice) 32 kbps to 1.5 Mbps (video)	BER 10^{-6}	10 ms
	Non-time-critical services: IP, IPX, frame relay, audio/video streaming, bulk data transfer, etc.	≤155 Mbps	BER 10^{-8}	N/A
	MPEG video	≤8 Mbps	BER 10^{-11}	TBD
Fixed-length Cell/Packet	ATM Cell Relay—CBR	16 kbps to 155 Mbps	CLR 3×10^{-8} CER 4×10^{-6} CMR 1/day SEBCR 10^{-4}	10 ms
	ATM Cell Relay—rt-VBR	16 kbps to 155 Mbps	CLR 10^{-5} CER 4×10^{-6} CMR 1/day SEBCR 10^{-4}	10 ms
	ATM Cell Relay—other	≤155 Mbps	CLR 10^{-5} CER 4×10^{-6} CMR 1/day SEBCR 10^{-4}	N/A

Table 11.10 summarizes requirements in three categories. The first category is the data rate that must be supported. The second category refers to error performance. For most services an upper limit on the bit error ration (BER) is defined. For ATM, various specific QoS error parameters are also used.

The final category is maximum one-way delay. To place this delay in context, Figure 11.13 shows three categories of delay defined in the 802.16 standards:

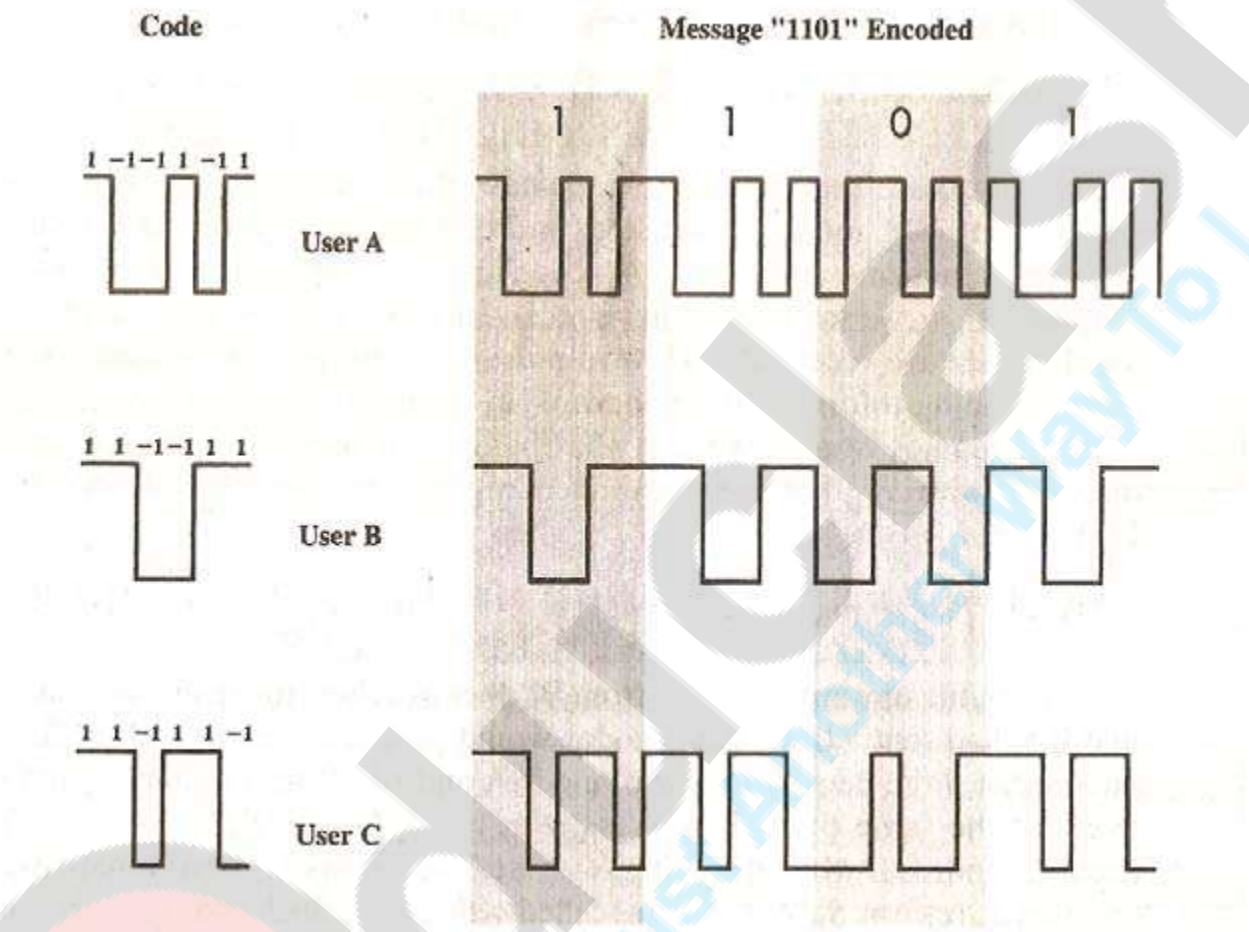
• Medium access delay: Once a transceiver station is ready to transmit, the medium access delay measures the amount of time that the station must wait before it can transmit.

• 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. The maximum one-way delay category specified in Table 11.10 refers to transit delay.

Q1 B) CDMA and WCDMA access technique ?
Ans: CDMA:



CDMA is a multiplexing technique used with spread spectrum. The scheme works i 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
cA = <1,-1,-1,1,-1,1>, similarly, user B has code cB = <1,1,-1,-1,1,1>, and user C has cC = <1,1,-1,1,1,-1>.

Consider the case of user A communicaing 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:
Su(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 SA becomes SA(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
SA(-1,1,1,-1,1,-1)= -6
Also SA is such that -6 <= SA(d) <= 6.

If SA 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 SA(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 SA again. This means that if the decoder is linear and if A and B transmit signals sA and sB, respectively, at the same time, then SA(sA + sB)=SA(sA)+SA(sB)=SA(sA) since the decoder ignores B when it is using A's code. The codes of A and B that have the property that SA(cB) = SB(cA) = 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.

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.

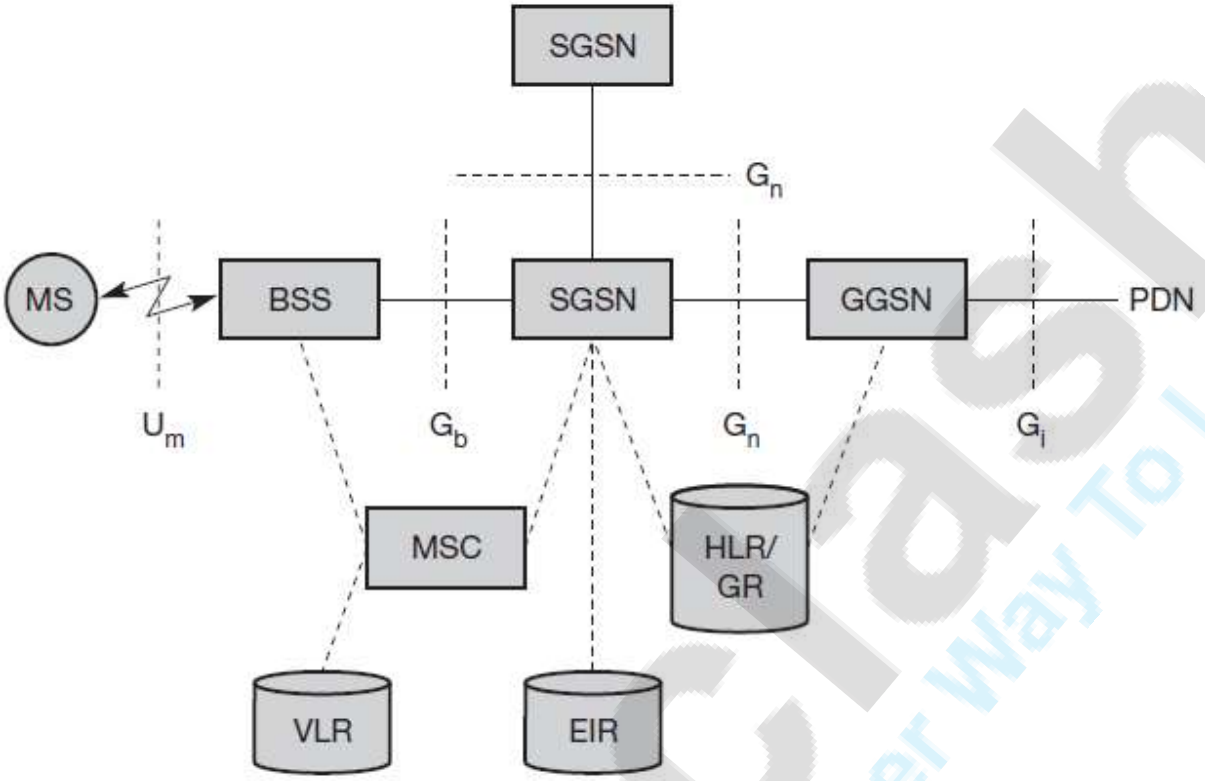
2. FDD: The uplink and downlink transmission employ two separated frequency bands for this duplex method. A pair of frequency bands with specified separation is assigned for connection.

Q2 A) What is 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 IPbased 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.



As shown in Figure, 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.

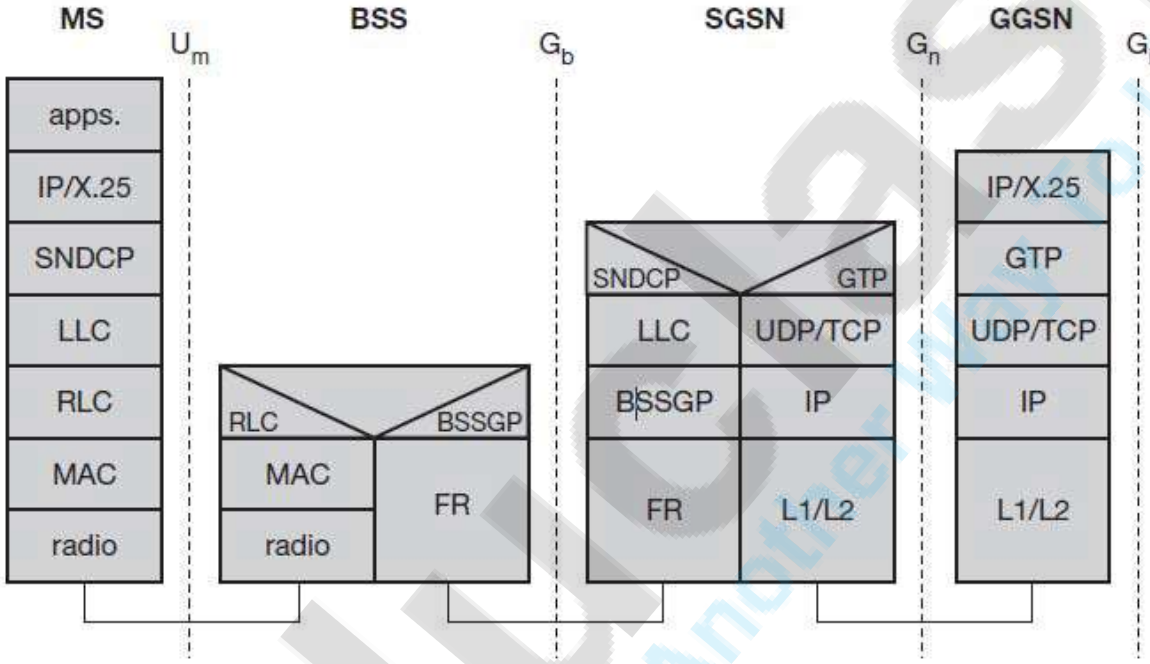


Figure shows the protocol architecture of the transmission plane for GPRS. Architectures for the signaling planes can be found in ETSI (1998b). All data within the GPRS backbone, i.e., between the GSNs, is transferred using the GPRS tunnelling protocol (GTP). GTP can use two different transport protocols, 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 ofSNDCP 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).

Q2 B) Explain briefly Antennas with example ?
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.

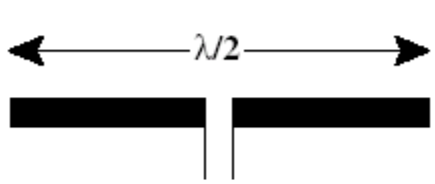
2. For the transmission of the signal, radio-frequency electrical energy from the transmitter is converted into electromagnetic energy by the antenna and radiated into the surrounding environment.

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

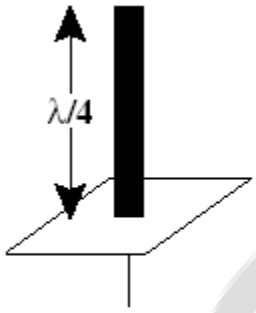
Antenna Types:

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.



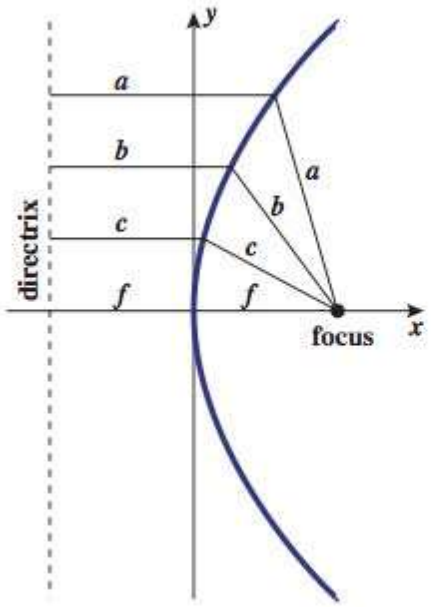
(a) Half-wave dipole



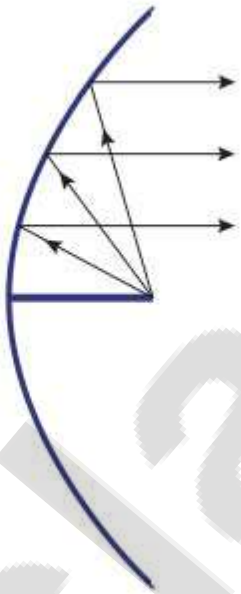
(b) Quarter-wave antenna

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:



(a) Parabola



(b) Cross-section of parabolic antenna showing reflective property

Q3 A) Describe different error-detecting and error-correcting codes used?

Ans 3 :

Error detection and correction has great practical importance in maintaining data (information) integrity across noisy Communication Networks channels and lessthan- reliable storage media.

Error Correction : Send additional information so incorrect data can be corrected and accepted. Error correction is the additional ability to reconstruct the original, error-free data.

There are two basic ways to design the channel code and protocol for an error correcting system :

• Automatic Repeat-Request (ARQ) : The transmitter sends the data and also an error detection code, which the receiver uses to check for errors, and request retransmission of erroneous data. In many cases, the request is implicit; the receiver sends an acknowledgement (ACK) of correctly received data, and the transmitter re-sends anything not acknowledged within a reasonable period of time.

• Forward Error Correction (FEC) : The transmitter encodes the data with an error-correcting code (ECC) and sends the coded message. The receiver never sends any messages back to the transmitter. The receiver decodes what it receives into the "most likely" data. The codes are designed so that it would take an "unreasonable" amount of noise to trick the receiver into misinterpreting the data.

Error Detection : Send additional information so incorrect data can be detected and rejected. Error detection is the ability to detect the presence of errors caused by noise or other impairments during transmission from the transmitter to the receiver.

Error Detection Schemes : In telecommunication, a redundancy check is extra data added to a message for the purposes of error detection. Several schemes exist to achieve error detection, and are generally quite simple. All error detection codes transmit more bits than were in the original data. Most codes are "systematic": the transmitter sends a fixed number of original data bits, followed by fixed number of check bits usually referred to as redundancy which are derived from the data bits by some deterministic algorithm.

Repetition Schemes : Variations on this theme exist. Given a stream of data that is to be sent, the data is broken up into blocks of bits, and in sending, each block is sent some predetermined number of times. For example, if we want to send

"1011", we may repeat this block three times each. Suppose we send "1011 1011 1011", and this is received as "1010 1011 1011".

Parity Schemes : A parity bit is an error detection mechanism . A parity bit is an extra bit transmitted with a data item, chose to give the resulting bitseven or odd parity. Parity refers to the number of bits set to 1 in the data item. There are 2 types of parity

- Even parity - an even number of bits are 1 Even parity - data: 10010001, parity bit 1
- Odd parity - an odd number of bits are 1 Odd parity - data: 10010111, parity bit 0

Checksum : A checksum of a message is an arithmetic sum of message code words of a certain word length, for example byte values, and their carry value. The sum is negated by means of ones-complement, and stored or transferred as an extra code word extending the message. On the receiver side, a new checksum may be calculated, from the extended message.

Hamming Distance Based Checks : If we want to detect d bit errors in an n bit word we can map every n bit word into a bigger n+d+1 bit word so that the minimum Hamming distance between each valid mapping is d+1. This way, if one receives n+d+1 bit word that doesn't match any word in the mapping (with a Hamming distance x <= d+1 from any word in the mapping) it can successfully detect it as an errored word. Even more, d or fewer errors will never transform a valid word into another, because the Hamming distance between each valid word is at least d+1, and such errors only lead to invalid words that are detected correctly.

cyclic redundancy check A cyclic redundancy check (CRC) or polynomial code checksum is a hash functiondesigned to detect accidental changes to raw computer data, and is commonly used in digital networks and storage devices such as hard disk drives. A CRC-enabled device calculates a short, fixed-length binary sequence, known as the CRC code or just CRC, for each block of data and sends or stores them both together. CRCs are so called because the check (data verification) code is a redundancy (it adds zero information to the message) and the algorithm is based on cyclic codes. The term CRC may refer to the check code or to the function that calculates it, which accepts data streams of any length as input but always outputs a fixed-length code.

Q3 B) What is the difference between soft hand-off and hard hand-off?
Ans-3b:
When a mobile user travels from one area of coverage or cell to another cell within a call's duration the call should be transferred to the new cell's base station. Otherwise, the call will be dropped because the link with the current base station becomes too weak as the mobile recedes. Indeed, this ability for transference is a design matter in mobile cellular system design and is call handoff.
hard handoff vs. soft handoff
Soft handover or soft handoff refers to a feature used by the CDMA and W-CDMA standards, where a cell phone is simultaneously connected to two or more cells (or cell sectors) during a call. If the sectors are from the same physical cell site (a sectorised site), it is referred to as softer handoff. This technique is a form of mobile-assisted handover, for IS-95/CDMA2000 CDMA cell phones continuously make power measurements of a list of neighboring cell sites, and determine whether or not to request or end soft handover with the cell sectors on the list.
On the uplink (phone-to-cell-site), all the cell site sectors that are actively supporting a call in soft handover send the bit stream that they receive back to the Radio Network Controller (RNC), along with information about the quality of the received bits. The RNC examines the quality of all these bit streams and dynamically chooses the bit stream with the highest quality. Again, if the signal degrades rapidly, the chance is still good that a strong signal will be available at one of the other cell sectors that is supporting the call insoft handover.
Hard handover In a mobile cellular communication network, a Hard handoff (or Hard handover) is a typicalHandoff mechanism in a communication network which is designed to work by first breaking off from the initial connection with a base station before switching to another base station. This is done in order to retain communications in a session for mobile users after incurring a non perceptible and insignificant brief interruption. A Hard handoff is also referred to as "Break-before-Make" handover.
A Hard handoff can be practically employed with more efficiency in FDMA (Frequency Division Multiple Access) and TDMA (Time Division Multiple Access) network access systems, because in these systems channel interference is minimized since different frequency ranges are used from adjacent channels. Mostly CDMA (Code Division Multiple Access)-based technologies employ Soft handoffs.
A Hard handoff mechanism is particularly suitable for delay-tolerant communication traffic such as in broadband technology-enabled Internet, VoIP,

mobile networking technology such as mobile WiMax. Broadband Internet access and emailing are more efficient and reliable when a Hard handoff mechanism is used.

Q4 A) What is Pico-net & scatter net?
Ans.

Piconet :

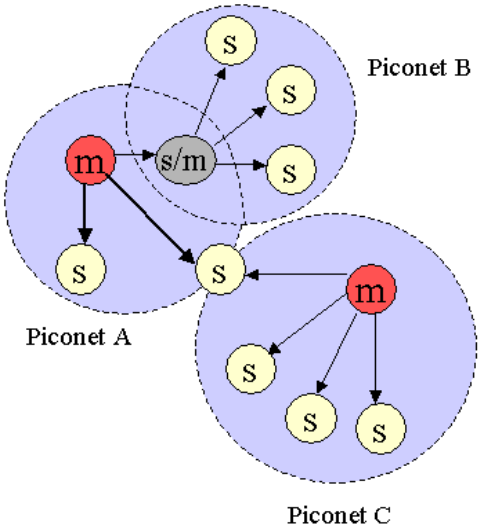
- A piconet is a network that is created using a wireless Bluetooth connection. A piconet consists of two or more devices occupying the same physical channel (synchronized to a common clock and hopping sequence).
- Some examples of piconets include a cell phone connected to a computer, a laptop and connected to Bluetooth-enabled digital camera, or several PDAs that are connected to each other.
- A piconet computer network linking a wireless user group of devices using Bluetooth technology protocols. It allows one master device to interconnect with up to seven activeslave devices.
- Up to 255 further slave devices can be inactive, or parked, which the master device can bring into active status at any time.
- A group of devices connected via Bluetooth technology in an ad hoc fashion. A piconet starts with two connected devices, and may grow to eight connected devices. Bluetooth communication always designates one of the Bluetooth devices as a main controlling unit or master unit.
- Other devices that follow the master unit are slave units. This allows the Bluetooth system to be non-contention based (no collisions). This means that after a Bluetooth device has been added to the piconet, each device is assigned a specific time period to transmit and they do not collide or overlap with other units operating within the same piconet.
- Piconet range varies according to the class of the Bluetooth device. Data transfer rates vary between about 200 and 2100 kilobits per second.
- Because the Bluetooth system hops over 79 channels, the probability of interfering with another Bluetooth system is less than 1.5%. This allows several Bluetooth Piconets to operate in the same area at the same time with minimal interference.
- The original piconet was a networking type used on Nimbus computers produced by RM plc.

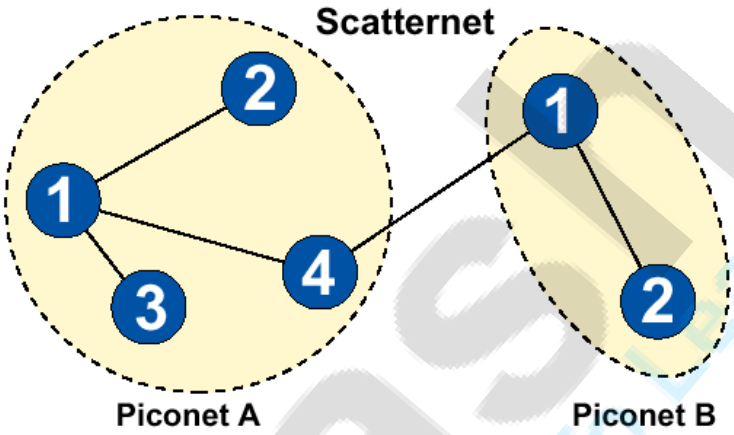
Scatter net :

- A scatternet is a type of ad hoc computer network consisting of two or more piconets. The terms 'scatternet' and 'piconet' are typically applied to Bluetooth wireless technology.

- A piconet is the type of connection that is formed between two or more Bluetooth-enabled devices such as modern cell phones or PDAs. Bluetooth enabled devices are "peer units" in that they are able to act as either master or slave.
- However, when a piconet is formed between two or more devices, one device takes the role of 'master', and all other devices assume a 'slave' role for synchronization reasons. Piconets have a 3-bit address space, which limits the maximum size of a piconet to 8 devices ($2^3 = 8$), i.e. 1 master and 7 slaves.
- A scatternet is a number of interconnected piconets that supports communication between more than 8 devices. Scatternets can be formed when a member of one piconet (either the master or one of the slaves) elects to participate as a slave in a second, separate piconet.
- The device participating in both piconets can relay data between members of both ad hoc networks. However, the basic bluetooth protocol does not support this relaying - the host software of each device would need to manage it. Using this approach, it is possible to join together numerous piconets into a large scatternet, and to expand the physical size of the network beyond Bluetooth's limited range.
- Currently there are very few actual implementations of scatternets due to limitations of Bluetooth and the MAC address protocol. However, there is a growing body of research being conducted with the goal of developing algorithms to efficiently form scatternets.
- Scatternets have the potential to bring the interconnectivity of the Internet to the physical world through wireless devices. A number of companies have attempted to launch social networking and dating services that leverage early scatternet implementations.
- Scatternets can also be used to enable ad hoc communication and interaction between autonomous robots and other devices.

Diagrammatically,





Q.4 B) Describe frequency hopping & direct sequence spread spectrum techniques.

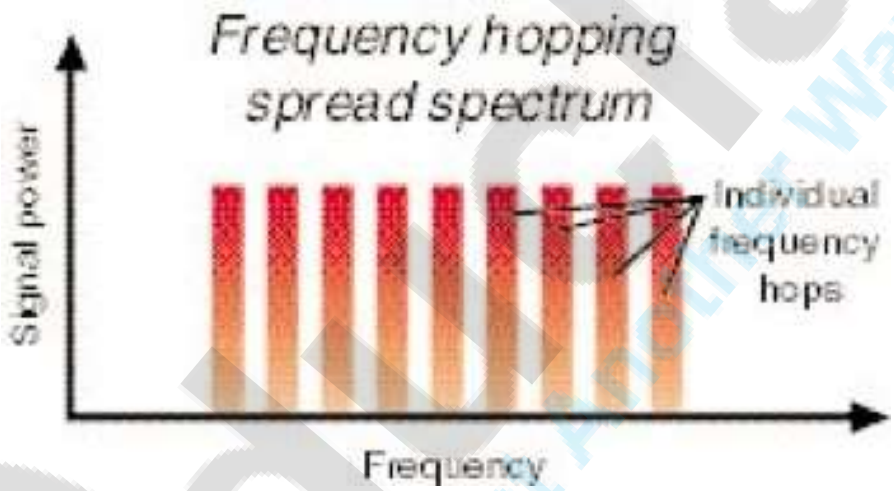
Ans.

Frequency-hopping spread spectrum (FHSS)

- It is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels, using pseudorandom sequence known to both transmitter and receiver.
- It is utilized as multiple in the frequency-hopping code division multiple access (FH-CDMA) scheme.
- Frequency hopping is one of two basic modulation techniques used in spread signal transmission. It is the repeated switching of frequencies during radio transmission, often to minimize the effectiveness of "electronic warfare" - that is, the unauthorized interception or jamming of telecommunications. It also is known as frequency- hopping code division multiple access (FH-CDMA).
- Spread spectrum modulation techniques have become more common in recent years. Spread spectrum enables a signal to be transmitted across a frequency band that is much wider than the minimum bandwidth required by the information signal.

- The transmitter "spreads" the energy, originally concentrated in narrowband, across a number of frequency band channels on a wider electromagnetic spectrum.
- Benefits include improved privacy, decreased narrowband interference, and increased signal capacity.
- In an FH-CDMA system, a transmitter "hops" between available frequencies according to a specified algorithm, which can be either random or preplanned.
- The transmitter operates in synchronization with a receiver, which remains tuned to the same center frequency as the transmitter. A short burst of data is transmitted on a narrowband. Then, the transmitter tunes to another frequency and transmits again.
- The receiver thus is capable of hopping its frequency over a given bandwidth several times a second, transmitting on one frequency for a certain period of time, then hopping to another frequency and transmitting again.
- Frequency hopping requires a much wider bandwidth than is needed to transmit the same information using only one carrier frequency.
- The spread spectrum approach that is an alternative to FH-CDMA is direct sequence code division multiple access (DS-CDMA), which chops the data into small pieces and spreads them across the frequency domain.
- FH-CDMA devices use less power and are generally cheaper, but the performance of DS-CDMA systems is usually better and more reliable.
- The biggest advantage of frequency hopping lies in the coexistence of several access points in the same area, something not possible with direct sequence.
- Certain rules govern how frequency-hopping devices are used. In North America, the Industrial, Scientific, and Medial (ISM) waveband is divided into 75 hopping channels, with power transmission not to exceed 1 watt on each channel.
- These restrictions ensure that a single device does not consume too much bandwidth or linger too long on a single frequency.
- The Federal Communications Commission (FCC) has amended rules to allow frequency hopping spread spectrum systems in the unregulated 2.4 GHz band.

- The rule change is designed to allow wider bandwidths, thus enabling Internet devices to operate at higher speeds and fostering development of wireless LANs and wireless cable modems.
- Movie star Hedy Lamarr is generally credited as co-originator of the idea of spread spectrum transmission. She and her pianist were issued a patent for the technique during World War II.
- They discovered the technique using a player piano to control the frequency hops, and envisioned it as a way to provide secure communications during wartime. The pair never made any money off the invention and their patent eventually expired.
- Sylvania introduced a similar concept in the 1950s and coined the term "spread spectrum."

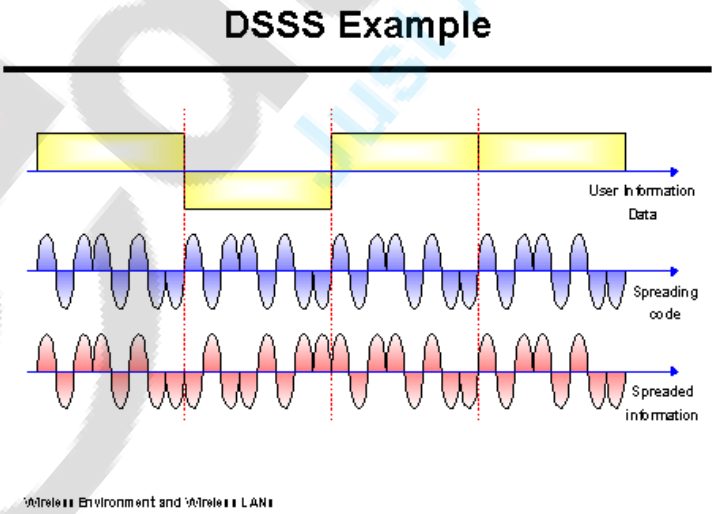


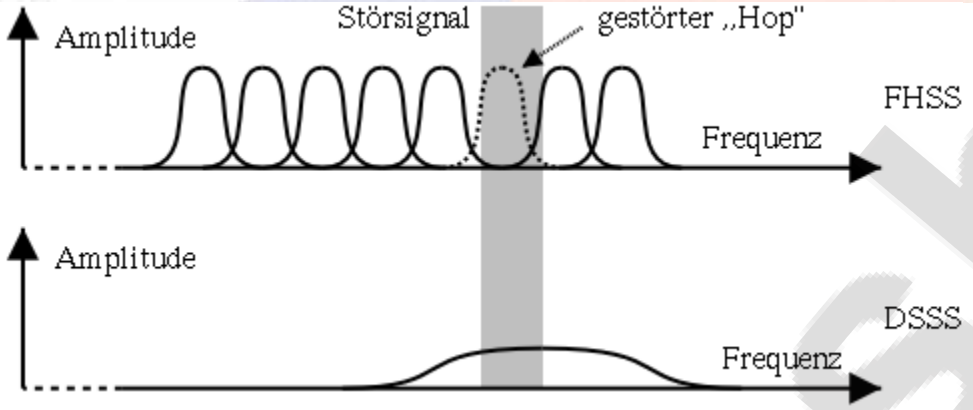
Direct-sequence spread spectrum (DSSS)

- It is a modulation technique. As with other spectrum technologies, the transmitted signal takes up more bandwidth than the information signal that modulates the carrier or broadcast frequency.
- The name 'spread spectrum' comes from the fact that the carrier signals occur over the full bandwidth (spectrum) of a device's transmitting frequency. Certain IEEE 802.11 standards use DSSS signaling.
- Direct sequence spread spectrum, also known as direct sequence code division multiple access (DS-CDMA), is one of two approaches to spread spectrum modulation for digital signal transmission over the airwaves.

- In direct sequence spread spectrum, the stream of information to be transmitted is divided into small pieces, each of which is allocated across to a frequency channel across the spectrum.
- A data signal at the point of transmission is combined with a higher data-rate bit sequence (also known as a chipping code) that divides the data according to a spreading ratio.
- The redundant chipping code helps the signal resist interference and also enables the original data to be recovered if data bits are damaged during transmission.
- Direct sequence contrasts with the other spread spectrum process, known as frequency hopping spread spectrum, or frequency hopping code division multiple access (FH-CDMA), in which a broad slice of the bandwidth spectrum is divided into many possible broadcast frequencies.
- In general, frequency-hopping devices use less power and are cheaper, but the performance of DS-CDMA systems is usually better and more reliable.
- Spread spectrum first was developed for use by the military because it uses wideband signals that are difficult to detect and that resist attempts at jamming.
- In recent years, researchers have turned their attention to applying spread spectrum processes for commercial purposes, especially in local area wireless networks.

FDSS vs DSSS





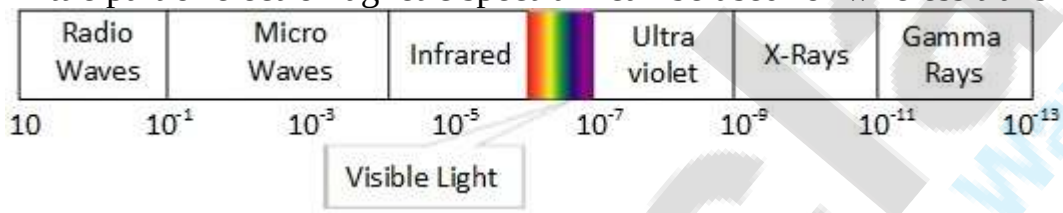
Q5 A) What is wireless transmission? Compare digital and analog transmission techniques?

Ans.

Wireless transmission is a form of unguided media. Wireless communication involves no physical link established between two or more devices, communicating wirelessly. Wireless signals are spread over in the air and are received and interpret by appropriate antennas.

When an antenna is attached to electrical circuit of a computer or wireless device, it converts the digital data into wireless signals and spread all over within its frequency range. The receptor on the other end receives these signals and converts them back to digital data.

A little part of electromagnetic spectrum can be used for wireless transmission.



Radio Transmission

Radio frequency is easier to generate and because of its large wavelength it can penetrate through walls and alike structures. Radio waves can have wavelength from 1 mm – 100,000 km and have frequency ranging from 3 Hz (Extremely Low Frequency) to 300 GHz (Extremely High Frequency). Radio frequencies are sub-divided into six bands.

Radio waves at lower frequencies can travel through walls whereas higher RF travel in straight line and bounces back. The power of low frequency waves decreases sharply as it covers longer distance

Microwave Transmission

Electromagnetic waves above 100 MHz tend to travel in a straight line and signals over them can be sent by beaming those waves towards one particular station. Because Microwaves travels in straight lines, both sender and receiver must be aligned to be strictly in line-of-sight.

Infrared Transmission

Infrared waves lies in between visible light spectrum and microwaves. It has wavelength of 700 nm to 1 mm and frequency ranges from 300 GHz to 430 THz.

Light Transmission

Highest most electromagnetic spectrum which can be used for data transmission is light or optical signaling. This is achieved by means of LASER.
Because of frequency light uses, it tends to travel strictly in straight line. So the sender and receiver must be in the line-of-sight

Two forms of transmission:
An **analog signal** is a continuously varying electromagnetic wave that may be propagated over a variety of media, depending on frequency; examples are copper wire media, such as twisted pair and coaxial cable
A **digital signal** is a sequence of voltage pulses that may be transmitted over a copper wire medium;for example, a constant positive voltage level may represent binary 0 and a constantnegative voltage level may represent binary l.

Comparison chart

	Analog	Digital
Signal	Analog signal is a continuous signal which represents physical measurements.	Digital signals are discrete time signals generated by digital modulation.
Waves	Denoted by sine waves	Denoted by square waves
Representation	Uses continuous range of values to represent information	Uses discrete or discontinuous values to represent information
Example	Human voice in air, analog electronic devices.	Computers, CDs, DVDs, and other digital electronic devices.
Technology	Analog technology records waveforms as they are.	Samples analog waveforms into a limited set of numbers and records them.
Data transmissions	Subjected to deterioration by noise during transmission and write/read cycle.	Can be noise-immune without deterioration during transmission and write/read cycle.
Response to Noise	More likely to get affected reducing accuracy	Less affected since noise response are analog in nature

	Analog	Digital
Flexibility	Analog hardware is not flexible.	Digital hardware is flexible in implementation.
Uses	Can be used in analog devices only. Best suited for audio and video transmission.	Best suited for Computing and digital electronics.
Applications	Thermometer	PCs, PDAs
Bandwidth	Analog signal processing can be done in real time and consumes less bandwidth.	There is no guarantee that digital signal processing can be done in real time and consumes more bandwidth to carry out the same information.
Memory	Stored in the form of wave signal	Stored in the form of binary bit
Power	Analog instrument draws large power	Digital instrument drawS only negligible power
Cost	Low cost and portable	Cost is high and not easily portable
Impedance	Low	High order of 100 megaohm
Errors	Analog instruments usually have a scale which is cramped at lower end and give considerable observational errors.	Digital instruments are free from observational errors like parallax and approximation errors.

Q6 B) Explain briefly XHTML with example?

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

XHTML documents are well-formed and may therefore be parsed using standard XML parsers, unlike HTML, which requires a lenient HTML-specific parser.

XHTML 1.0 became a World Wide Web Consortium (W3C) Recommendation on January 26, 2000. XHTML 1.1 became a W3C Recommendation on May 31, 2001. The standard known as XHTML5 is being developed as an XML adaptation of the HTML5 specification

XHTML 1.0 is "a reformulation of the three HTML 4 document types as applications of XML 1.0". The World Wide Web Consortium (W3C) also continues to maintain the HTML 4.01 Recommendation, and the specifications for HTML5 and XHTML5 are being actively developed

Motivation

XHTML was developed to make HTML more extensible and increase interoperability with other data formats. HTML 4 was ostensibly an application of Standard Generalized Markup Language (SGML); however the specification for SGML was complex, and neither web browsers nor the HTML 4 Recommendation were fully conformant to it.

Versions of XHTML

XHTML 1.0

In earlier times[when?], Wikipedia used the XHTML 1.0 Transitional doctype and syntax, though it was not served as XHTML

December 1998 saw the publication of a W3C Working Draft entitled Reformulating HTML in XML. This introduced Voyager, the codename for a new markup language based on HTML 4, but adhering to the stricter syntax rules of XML. By February 1999 the name of the specification had changed to XHTML 1.0: The Extensible HyperText Markup Language, and in January 2000 it was officially adopted as a W3C Recommendation. There are three formal DTDs for XHTML 1.0, corresponding to the three different versions of HTML 4.01:

- XHTML 1.0 Strict is the XML equivalent to strict HTML 4.01, and includes elements and attributes that have not been marked deprecated in the HTML 4.01 specification. As of May 25, 2011, XHTML 1.0 Strict is the document type used for the homepage of the website of the World Wide Web Consortium.

- XHTML 1.0 Transitional is the XML equivalent of HTML 4.01 Transitional, and includes the presentational elements (such as center, font and strike) excluded from the strict version.
- XHTML 1.0 Frameset is the XML equivalent of HTML 4.01 Frameset, and allows for the definition of frameset documents—a common Web feature in the late 1990s.

The second edition of XHTML 1.0 became a W3C Recommendation in August 2002.

Semantic content in XHTML

XHTML+RDFa is an extended version of the XHTML markup language for supporting RDF through a collection of attributes and processing rules in the form of well-formed XMLdocuments. This host language is one of the techniques used to develop Semantic Web content by embedding rich semantic markup.

DOCTYPEs

Main article: DOCTYPE

In order to validate an XHTML document, a Document Type Declaration, or DOCTYPE, may be used. A DOCTYPE declares to the browser the Document Type Definition (DTD) to which the document conforms. A Document Type Declaration should be placed before the root element.

Common errors

Not closing empty elements

- Incorrect:
- Correct:

Omitting end tags

- Incorrect: This is a paragraph. This is another paragraph.
- Correct: This is a paragraph. This is another paragraph.
- Improperly nesting elements (Note that this would also be invalid in HTML)
- Incorrect: This is some text.
- Correct: This is some text.
- Using attribute minimization
- Incorrect: <textarea readonly>READ-ONLY</textarea>
- Correct: <textarea readonly="readonly">READ-ONLY</textarea>

Backward compatibility

XHTML 1.x documents are mostly backward compatible with HTML 4 user agents when the appropriate guidelines are followed

Examples

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
 <head>
 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
 <title>XHTML 1.0 Strict Example</title>
 <script type="text/javascript">
 //<![CDATA[
 function loadpdf() {
    document.getElementById("pdf-
object").src="http://www.w3.org/TR/xhtml1/xhtml1.pdf";
 }
 //]]>
 </script>
 </head>
 <body onload="loadpdf()">
 <p>This is an example of an
 <abbr title="Extensible HyperText Markup Language">XHTML</abbr> 1.0 Strict
document.<br />
 <img id="validation-icon"
    src="http://www.w3.org/Icons/valid-xhtml10"
    alt="Valid XHTML 1.0 Strict" /><br />
 <object id="pdf-object"
    name="pdf-object"
    type="application/pdf"
    data="http://www.w3.org/TR/xhtml1/xhtml1.pdf"
    width="100%"
    height="500">
 </object>
 </p>
 </body>
</html>
```

Q6 A) What is Fading? Explain the types of fading how does fading effect the wireless transmission?

Ans.

In wireless communications, fading is deviation of the attenuation affecting a signal over certain propagation media. The fading may vary with time,

geographical position or radio frequency, and is often modeled as a random process. A fading channel is a communication channel comprising 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.

Types:
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 or phase change of the channel to become uncorrelated from 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 received power 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.

Mitigation:
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.

Diversity can be achieved in time, frequency, or space. Common techniques used to overcome signal fading include:

Diversity reception and transmission
MIMO
OFDM
Rake receivers
Space–time codes

Q6. B) What is difference between Palm OS and Symbian OS?

Ans.

- Palm OS is an embedded operating system designed for ease of use with a touchscreen-based graphical user interface.
- It has been implemented on a wide variety of mobile devices such as smart phones, barcode readers, and GPS devices.
- It is run on Arm architecture-based processors. It is designed as a 32-bit architecture.

The key features of Palm OS are:

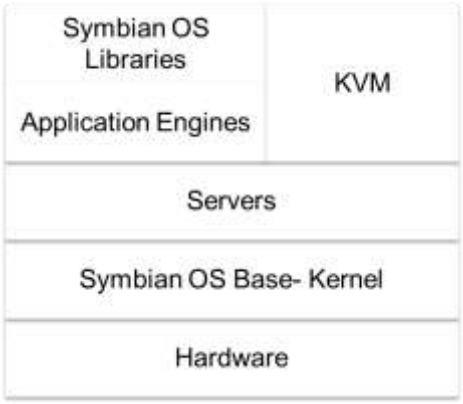
- A single-tasking OS:
- Palm OS Garnet (5.x) uses a kernel developed at Palm, but it does not expose tasks or threads to user applications. In fact, it is built with a set of threads that cannot be changed at runtime.
- Palm OS Cobalt (6.0 or higher) does support multiple threads but does not support creating additional processes by user applications.
- Palm OS has a preemptive multitasking kernel that provides basic tasks but it does not expose this feature to user applications.
- Memory Management:
- The Memory, RAM and ROM, for each Palm resides on a memory module known as card. In other words, each memory card contains RAM, ROM or both. Palms can have no card, one card or multiple cards.
- Expansion support:
- This capability not only augments the memory and I/O, but also it facilitates data interchanges with other Palm devices and with other non-Palm devices such as digital cameras, and digital audio players.
- Handwriting recognition input called Graffiti
- HotSync technology for synchronization with PC computers
- Sound playback and record capabilities
- TCP/IP network access
- Support of serial port, USB, Infrared, Bluetooth and Wi-Fi connections
- Defined standard data format for PIM (Personal Information Management) applications to store calendar, address, task and note entries, accessible by third-party applications
- Security model:

- Device can be locked by password, arbitrary application records can be made private
- Palm OS Cobalt include a certificate manager. The Certificate Manager handles X.509 certificates.

Symbian OS:

- Symbian OS is 32 bit, little-endian operating system, running on different flavors of ARM architecture.
- It is a multitasking operating system and very less dependence on peripherals.
- Kernel runs in the privileged mode and exports its service to user applications via user libraries.
- User libraries include networking, communication, I/O interfaces and etc.
- Access to these services and resources is coordinated through a client-server framework.
- Clients use the service APIs exposed by the server to communicate with the server.
- The client-server communication is conducted by the kernel.

- The following demonstrates the Symbian OS architecture:



- Real-time: it has a real-time, multithreaded kernel.
- Data Caging: it allows applications to have their own private data partition. This feature allows for applications to guarantee a secure data store. It can be used for e-commerce applications, location aware applications and etc.
- Multimedia: it supports audio, video recording, playback and streaming, and Image conversion.
- Platform Security: Symbian provides a security mechanism against malware. It allows sensitive operations can be accessed by applications which have been certified by a signing authority. In addition, it supports full encryption and certificate management, secure protocols (HTTPS, TLS and SSL) and WIM framework.
- Internationalization support: it supports Unicode standard.
- Fully object-oriented and component- based
- Optimized memory management
- Client- server architecture: described in previous slides, it provides simple and high-efficient inter-process communication. This feature also eases porting of code written for other platforms to Symbian OS.
- A Hardware Abstraction Layer (HAL): This layer provides a consistent interface to hardware and supports device-independency
- Kernel offers hard real-time guarantees to kernel and user mode threads.

Q7) Write on:

1. Wi-Fi?

Ans. Wi-Fi, also spelled Wifi or WiFi, is a local area wireless technology that allows an electronic device to exchange data or connect to the internet using 2.4 GHz UHF and 5 GHz SHF radio waves. The name is a trademark name, and is a play on the audiophile term Hi-Fi. The Wi-Fi Alliance defines Wi-Fi as any "wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards". However, since most modern WLANs are based on these standards, the term "Wi-Fi" is used in general English as a synonym for "WLAN". Only Wi-Fi products that complete Wi-Fi Alliance interoperability certification testing successfully may use the "Wi-Fi CERTIFIED" trademark.

Many devices can use Wi-Fi, e.g., personal computers, video-game consoles, smartphones, digital cameras, tablet computers and digital audio players. These can connect to a network resource such as the Internet via a wireless network access point. Such an access point (or hotspot) has a range of about 20 meters (66 feet) indoors and a greater range outdoors. Hotspot coverage can comprise an area as small as a single room with walls that block radio waves, or as large as many square kilometres achieved by using multiple overlapping access points. Depiction of a device sending information wirelessly to another device, both connected to the local network, in order to print a document.

Wi-Fi can be less secure than wired connections (such as Ethernet) because an intruder does not need a physical connection. Web pages that use SSL are secure but unencrypted internet access can easily be detected by intruders. Because of this, Wi-Fi has adopted various encryption technologies. The early encryption WEP, proved easy to break. Higher quality protocols (WPA, WPA2) were added later. An optional feature added in 2007, called Wi-Fi Protected Setup (WPS), had a serious flaw that allowed an attacker to recover the router's password. The Wi-Fi Alliance has since updated its test plan and certification program to ensure all newly certified devices resist attacks.

2. Block Codes:

Ans. A block code of size k over an finite alphabet with q symbols {0, 1, 2, _, q-1} is a set of k
q-ary sequences of length n called codewords.
A message u = (u0, u1, u2, ..., uk-1), code word v = (v0, v1, v2,...., vn-1)
v1∞n = u1∞k ∞ Gk∞n
where ui, vi ∈ GF(q) and v ∈ GF(q)n
v does not depend on past u, memoryless
There are qk possible code words of length n, they are called q-ery (n, k) block code.
The Code rate is defined as R = k/n.
Example: Binary (7, 4) linear block code
Table 1: A Binary (7, 4) linear block code

(0 0 0 0) (0 0 0 0 0 0 0)
(1 0 0 0) (1 1 0 1 0 0 0)
(0 1 0 1) (0 1 1 0 1 0 1)
(1 1 0 0) (1 0 1 1 1 0 0)
(0 0 1 0) (1 1 1 0 0 1 0)
(1 0 1 0) (0 0 1 1 0 1 0)
(0 1 1 0) (1 0 0 0 1 1 0)
(1 1 1 0) (0 1 0 1 1 1 0)
(0 0 0 1) (1 0 1 0 0 0 1)
(1 0 0 1) (0 1 1 1 0 0 1)
(0 1 0 1) (1 1 0 0 1 0 1)
(1 1 0 1) (0 0 0 1 1 0 1)
(0 0 1 1) (0 1 0 0 0 1 1)
(1 0 1 1) (1 0 0 1 0 1 1)
(0 1 1 1) (0 0 1 0 1 1 1)
(1 1 1 1) (1 1 1 1 1 1 1)

3. WAP

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 that uses the protocol.
- The WAP Forum dates from 1989. It aimed primarily to bring together the various wireless technologies in a standardized protocol.
- The first company to launch a WAP site was Dutch mobile phone operator Telfort BV in October 1999. The site was developed as a side project by Christopher Bee and Euan McLeod and launched with the debut of the Nokia 7110
- In 2002 the WAP Forum was consolidated (along with many other forums of the industry) into Open Mobile Alliance (OMA]).
- 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)	WAP protocol suite
Wireless Session Protocol (WSP)	
Wireless Transaction Protocol (WTP)	
Wireless Transport Layer Security (WTLS)	
Wireless Datagram Protocol (WDP)	
*** Any Wireless Data Network ***	

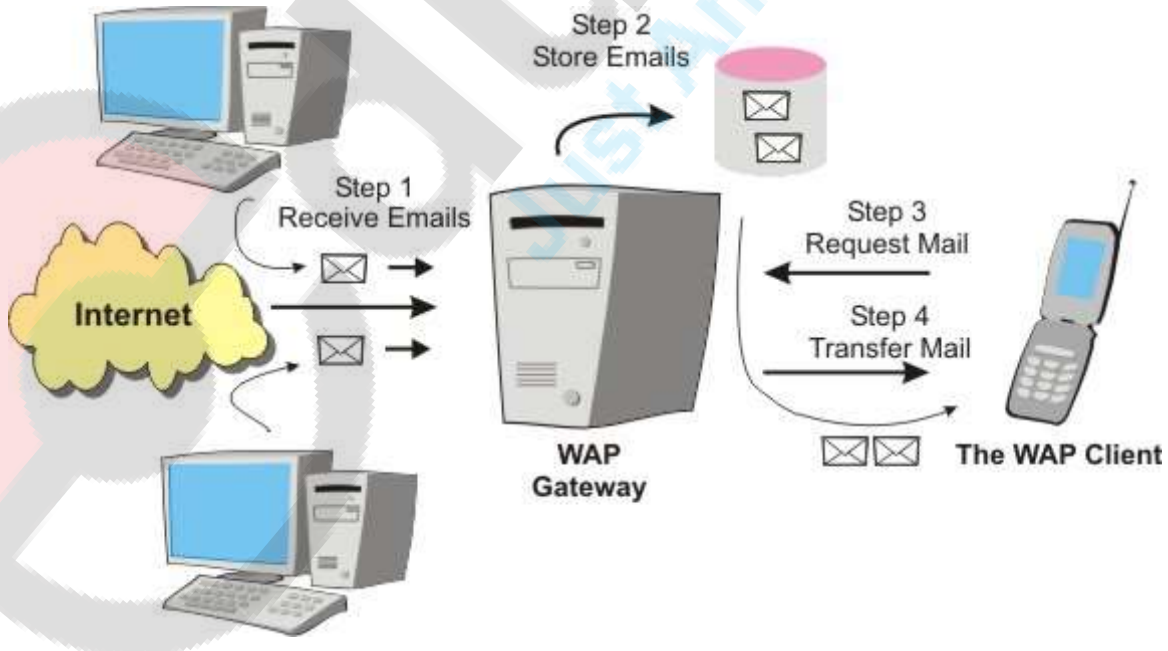
- The bottom-most protocol in the suite, the WAP Datagram Protocol (WDP), functions as an adaptation layer that makes every data network look a bit

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.

Diagrammatically,



4) TAPI

Ans.

The Telephony Application Programming Interface (TAPI) is a Microsoft Windows API, which provides computer telephony integration and enables PCs running Microsoft Windows to use telephone services.

TAPI was introduced in 1993 as the result of joint development by Microsoft and Intel. The first publicly available version of TAPI was version 1.3,

Different versions of TAPI are available on different versions of Windows. TAPI allows applications to control telephony functions between a computer and telephone network for data, fax, and voice calls. It includes basic functions, such as dialing, answering, and hanging up a call. It also supports supplementary functions, such as hold, transfer, conference, and Call Park found in PBX, ISDN, and other telephone systems.

TAPI is used primarily to control either modems or, more recently, to control business telephone system (PBX) handsets. When controlling a PBX handset, the driver is provided by the manufacturer of the telephone system

TAPI can also be used to control voice-enabled telephony devices, including voice modems and dedicated hardware such as Dialogic cards.

TAPI 2.x vs TAPI 3.x

TAPI 2.x and earlier versions were written in C; the API uses pointers to structures. Consequently, TAPI 2.x is easy to access from C or C++ applications, but it can be awkward to use from many other programming languages.

TAPI 3.x was designed with a Component Object Model (COM) interface. This was done with the intent of making it accessible to higher level applications such as developed inVB or other environments that provide easy access to COM but don't deal with C-style pointers.

TAPI 3.x has a slightly different set of functionality than TAPI 2.x. The addition of integrated media control was the most significant addition. But TAPI 3.x doesn't include all functionality that TAPI 2.x does, like support for the Phone class.

One very notable issue with TAPI 3.x is the lack of support for managed code (.NET environment). As documented in Microsoft KB Article 841712, Microsoft currently has no plans to support TAPI 3.x directly from .Net programming languages.

One often overlooked reason an application developer might choose between TAPI 2.x and TAPI 3.x should be the hardware vendors recommendation. Even though TAPI provides an abstract model of phone lines, telephony applications are still heavily impacted by the specific behavior of the underlying hardware.