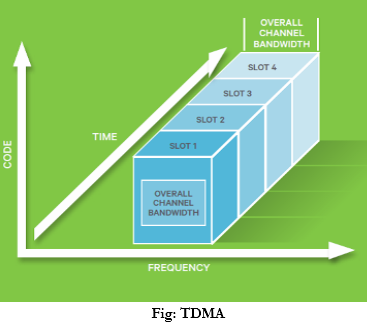
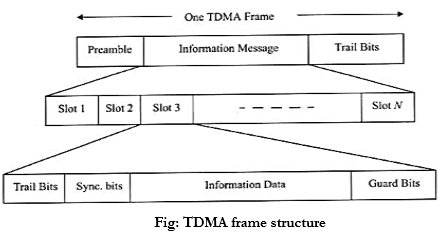
Q1: Explain in detail TDMA, CDMA and FDMA or Write short note on: Multiple access techniques.

Ans: **TDMA:**

It stands for time division multiple access.



* It uses time instead of frequency. Different users share same time slots of the complete time available.
* Each user is allocated a time slot in which user can access the channel.
* Transmission of data is in “burst and buffer” method. The transmission from different users is interfaced into repeating frame structure.



A frame consists of a no of slots. Each frame consists of preamble, an information message and trail bits. Half of the time slots are used for forward link channels and remaining for reverse link channels.

Guard bits are used to provide synchronization of different receivers between different time slots and frames.

* Guard time needs to be minimized
* Transmission rates are high.
* Handoff process is simple.

**CDMA:**

It stands for Code division multiple access.



* Users share the same carrier frequency(fc). The narrow band message signal is also multiplexed with a spreading signal of larger bandwidth. This spreading signal is pseudo noise code sequence and it has higher chip rate than rate of message.
* The main advantage is reduced level of interference. As each user is allocated an individual pseudo random codeword that is orthogonal to the codewords of the other users that the receiver end receives, tunes to receive the intended signal of the user.
* Same channel is used by several users, there may be a problem of near-far-effect. To reduce this power control is implemented at the base station.

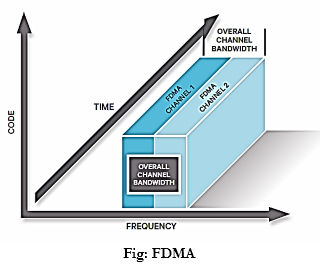
**Features:**

* Self-jamming is a problem
* Soft handoff is done
* Multipath fading can be reduced as signal is spread over a large spectrum.

**FDMA:**

It stands for Frequency division multiple access.

* The entire allocated radio spectrum is divided into many slices of the frequency bands and each band or channel is allocated to user. The channel allocation can be done on a demand basis to the users to request service.
* When a call is processed, no other user can share the same channel.



* Users are assigned a pair of frequencies, one for forward channel and other for reverse channel.

**Features:**

* No synchronization necessary
* Complexity of system is low
* All stations can operate continuously 24 hours without having to wait for their turn to come.
* Hard handover is done

**4. CSMA/CA:**

CSMA/CA [protocol](http://ecomputernotes.com/computernetworkingnotes/computer-network/protocol) is used in wireless networks because they cannot detect the collision so the only solution is collision avoidance.

• CSMA/CA avoids the collisions using three basic techniques.

(i) Interframe space

(ii) Contention window

(iii) Acknowledgements

****

The station ready to transmit, senses the line by using one of the persistent strategies.

* 1. As soon as it find the line to be idle, the station waits for an IFG (Interframe gap) amount of time.
  2. If then waits for some random time and sends the frame.
  3. After sending the frame, it sets a timer and waits for the acknowledgement from the receiver.
  4. If the acknowledgement is received before expiry of the timer, then the transmission is successful.
  5. But if the transmitting station does not receive the expected acknowledgement before the timer expiry then it increments the back off parameter, waits for the back off time and re senses the line.

**5. Polling Protocol:**

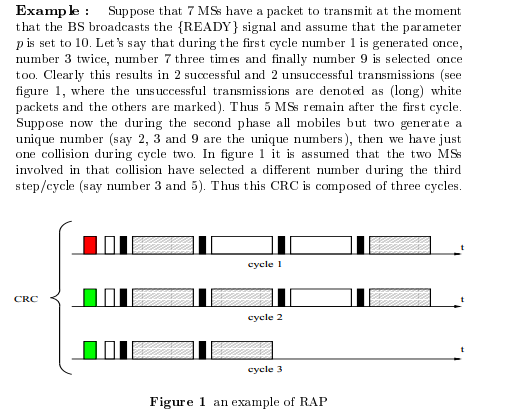
Randomly Addressed Polling (RAP):-

1. When a base station (BS) is ready to receive packets in the uplink direction it broadcasts a a READY signal to all the mobile stations (MS) in its area.

2. Each active MS (i.e. an MS ready to transmit a packet) generates a random number between 1 and p, p being a protocol parameter. The active MSs transmit these numbers simultaneously using CDMA (by means of p orthogonal codes) or using FDMA (by means of p di  
erent frequencies).

3. After receiving these numbers, the BS polls the active mobiles by transmitting the received numbers one **by one, and thus giving permission to use the uplink channel to transmit a packet. In case more than one MS has generated the same number, these MSs transmit a packet simultaneously and a collision occurs**. Acknowledgements are used to inform the mobile(s) whether the transmission was successful or not.

4. Steps 1 to 3, referred to as a pol ling cycle, are repeated for all unsuccessfully polled MSs, until all active MSs have sent their packet successfully (a different signal is used in step one to indicate that not all collisions were resolved).



**Q2: Why is the concept of spread spectrum important? Briefly explain FHSS and DSSS concepts.**

**Or Write short note on FHSS vs DHSS Or: Explain FHSS and DSSS with suitable example**

**Ans:- Spread Spectrum Definition**:- Spread spectrum is a technique used for transmitting radio or telecommunications signals. The term refers to the practice of spreading the transmitted signal to occupy the frequency spectrum available for transmission.

**The advantages of spectrum spreading**:-

1. access of same radio spectrum by multiple users (multiple access),

2. anti-jamming capability (so that signal transmission can not be interrupted or blocked by spurious transmission from enemy),

3. interference rejection,

4. secure communications,

5. multi-path protection

**Direct Sequence spread spectrum:**

Direct Sequence Spread Spectrum (DSSS) is a transmission technology used in wireless transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chippin sequence (code), that divides the user data according to a spreading factor (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 redundanc of the transmission.

**Advantages of DSSS**:

1. More restance to fading and multi-path effects
2. More efficient use of channel bandwidth
3. Short latency time
4. Constant processing gain - a better signal to noise ratio
5. Quick Lock-In as radio synchronize
6. No resynchronization with other radio necessary
7. Long outdoor range
8. Greater overall data throughput

**Disadvantage of DSSS:**

1. Complex design
2. Frequency hopping spread spectrum:

**Frequency Hopping Spread Spectrum (FHSS)** :

It is a transmission technology used in wireless 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. I synchronized properly, a single logical channel is maintained.

**Advantage of FHSS:**

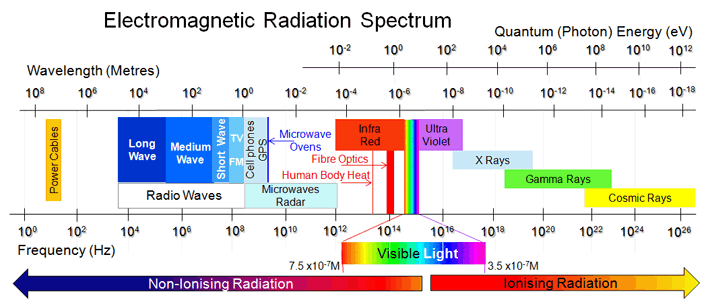
1. Fundamentally much simpler to implement
2. Better range, due to lower receiver sensitivity
3. Good rejection of in band interference
4. Good performance in multipath environments
5. No "near/far" problems

**Disadvantages of FHSS**:

1. Long latency time
2. Slow Lock-In, must search a channel
3. No processing gain
4. Must resynchronization with other after every hop
5. short outdoor range
6. Lower overall data throughput

**Q3: With a neat diagram explain electromagnetic spectrum. List the advantages and disadvantages of wireless technology****.**

**Electromagnetic spectrum**.  
[Electromagnetic spectrum](http://www.physics-and-radio-electronics.com/physics/electromagnetic-spectrum.html) is the range of all the frequencies or wavelengths of electromagnetic radiation.  
**Electromagnetic radiation.**Electromagnetic radiation is a form of energy in which electric, magnetic fields are mutually perpendicular to each other, and these two electric, and magnetic fields are perpendicular to the direction of wave propagation.



**1.** [**Radio waves**](http://www.physics-and-radio-electronics.com/physics/electromagnetic-spectrum/radio-waves.html) **:-**

[Radio waves](http://www.physics-and-radio-electronics.com/physics/electromagnetic-spectrum/radio-waves.html) has the longest wavelength and are mainly used for fixed and mobile radio communication.

Radio waves have the wavelength ranging from 1mm to 100km and frequencies ranging from 3KHZ to 300GHZ

**2. Microwaves:-**  
[Microwaves](http://www.physics-and-radio-electronics.com/physics/electromagnetic-spectrum/microwaves.html)are used in microwave ovens, telemetry, and radar. Microwaves have the wavelength ranging from 10 micrometer to 10 meter.

**3. Infrared rays:-**  
[Infrared rays](http://www.physics-and-radio-electronics.com/physics/electromagnetic-spectrum/infrared-radiation.html) are used in cameras for night vision and in medical treatments.

**4. Ultraviolet light:**  
[Ultraviolet light](http://www.physics-and-radio-electronics.com/physics/electromagnetic-spectrum/ultraviolet-light.html) is used to kill bacteria and other microbes.

**5.X-rays**  
[X-rays](http://www.physics-and-radio-electronics.com/physics/electromagnetic-spectrum/x-rays.html) are used to identify the bone fractures by passing radiation into internal body.

**6. Gamma rays:-**

Gamma rays are used to kill cancerous cells.

**Wireless technology:** - Wireless technology is an electromagnetic transmission medium that does not require a cable that is emitted through the medium of the air by a wave frequencies that can be used by the satellite, infrared rays, as well as satellites. With the wireless technology make people easier to do things with distances though.

**Wireless technology advantages**

1 Wireless technology really allows a network to reach locations that could not be achieved by using a network cable.

2. With the wireless system can provide the user with various access information in real-time anywhere. Given this extremely supportive in productivity and an increase in kualias than using a wired network.

3. Next advantages is the ease of installation. You do not necessarily need a cable to connect two or more computers. Then the installation process it will be much easier and lighter without stalling cable or perforate the wall.

4. A wireless LAN system can be configured with a variety of network topologies to meet the needs of the user. Himself the configuration can be changed from peer to peer with a small number of users to full infrastructure networks with up to thousands of users, and so allows for roaming in a large area.

5. Less [cost](http://wiki.answers.com/Q/What_are_the_advantages_and_disadvantages_of_wireless_communication) for cabling infrastructure and device

**Disadvantages Wireless**

1. Relatively lower bandwidth [speed](http://wiki.answers.com/Q/What_are_the_advantages_and_disadvantages_of_wireless_communication) – example: although currently 802.11/n could reach 128 Mbps, UTP cable can reach 1 Gbps. And more user mean each bandwidth get smaller. That is why currently wired backbone network is still preferred.

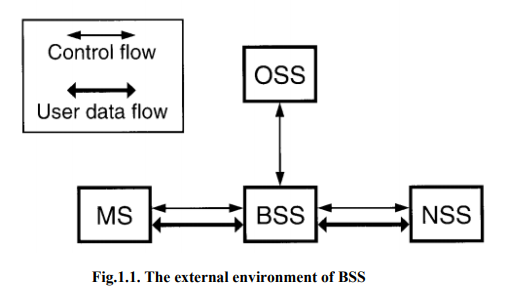
2. Ease of access means more security also necessary to [protect data](http://wiki.answers.com/Q/What_are_the_advantages_and_disadvantages_of_wireless_communication) and/or bandwidth, since people can connect anywhere within range without seeking network plug

**2 Cellular Network**

**Q1: Explain in detail GSM architecture.**

**Or Explain in detail Functional Architecture of a GSM system.**

**Ans:- GSM Architecture :** GSM consists of many subsystems, such as the mobile station (MS), the base station sub system (BSS), the network and switching subsystem (NSS), and the operation subsystem (OSS) in fig.1.1.



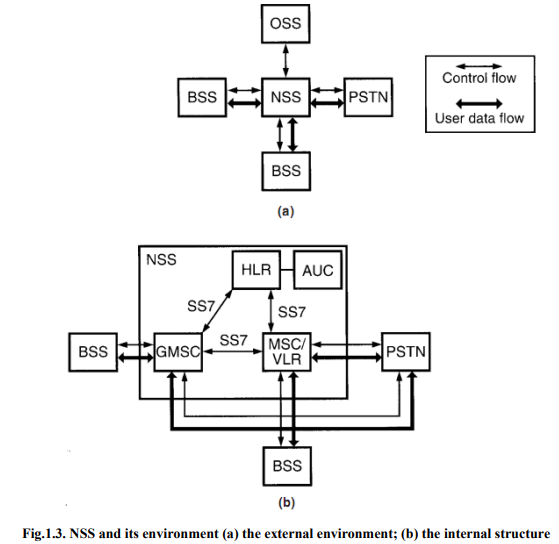
**1. The Mobile Station:** The MS may be a stand-alone piece of equipment for certain services or support the connection of external terminals, such as the interface for a personal computer or fax. The MS includes mobile equipment (ME) and a subscriber identity module (SIM). ME does not need to be personally assigned to one subscriber. The SIM is a subscriber module which stores all the subscriber-related information. When a subscriber’s SIM is inserted into the ME of an MS, that MS belongs to the subscriber, and the call is delivered to that MS. The ME is not associated with a called number—it is linked to the SIM. In this case, any ME can be used by a subscriber when the SIM is inserted in the ME.

**2. Base Station Subsystem**: The BSS connects to the MS through a radio interface and also connects to the NSS. The BSS consists of a base transceiver station (BTS) located at the antenna site and a base station controller (BSC) that may control several BTSs. The BTS consists of radio transmission and reception equipment similar to the ME in an MS. A transcoder/rate adaption unit (TRAU) carries out encoding and speech decoding and rate adaptation for transmitting data. As a subpart of the BTS, the TRAU may be sited away from the BTS, usually at the MSC. In this case, the low transmission rate of speech code channels allows more compressed transmission between the BTS and the TRAU, which is sited at the MSC. GSM uses the open system interconnection (OSI). There are three common interfaces based on OSI (Fig. 1.2.): a common radio interface, called air interface, between the MS and BTS, an interface A between the MSC and BSC, and an A-bis interface between the BTS and BSC. With these common interfaces, the system operator can purchase the product of manufacturing company A to interface with the product of manufacturing company B. The difference between interface and protocol is that an interface represents the point of contact between two adjacent entities (equipment or systems) and a protocol provides information flows through the interface. For example, the GSM radio interface is the transit point for information flow pertaining to several protocols.

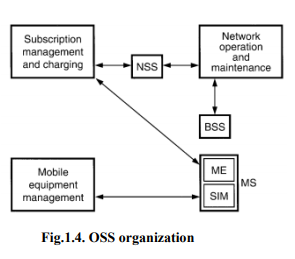


3. **Network and Switching Subsystem:** NSS (see Fig.1.3.) in GSM uses an intelligent network (IN). The IN’s attributes will be described later. A signaling NSS includes the main switching functions of GSM. NSS manages the communication between GSM users and other telecommunications users. NSS management consists of: Mobile service switching center (MSC): Coordinates call set-up to and from GSM users. An MSC controls several BSCs. Interworking function (IWF): A gateway for MSC to interface with external networks for communication with users outside GSM, such as packet-switched public data network (PSPDN) or circuit-switched public data network (CSPDN).The role of the IWF depends on the type of user data and the network to which it interfaces. Home location register (HLR): Consists of a stand-alone computer without switching capabilities, a database which contains subscriber information, and information related to the subscriber’s current location, but not the actual location of the subscriber. A subdivision of HLR is the authentication center (AUC). The AUC manages the security data for subscriber authentication. Another sub-division of HLR is the equipment identity register (EIR) which stores the data of mobile equipment (ME) or ME-related data. Visitor location register (VLR): Links to one or more MSCs, temporarily storing subscription data currently served by its corresponding MSC, and holding more detailed data than the HLR. For example, the VLR holds more current subscriber location information than the location information at the HLR.

Gateway MSC (GMSC): In order to set up a requested call, the call is initially routed to a gateway MSC, which finds the correct HLR by knowing the directory number of the GSM subscriber. The GMSC has an interface with the external network for gatewaying, and the network also operates the full Signaling System 7 (SS7) signaling between NSS machines. Signaling transfer point (STP): Is an aspect of the NSS function as a stand-alone node or in the same equipment as the MSC. STP optimizes the cost of the signaling transport among MSC/VLR, GMSC, and HLR. As mentioned earlier, NSS uses an intelligent network. It separates the central data base (HLR) from the switches (MSC) and uses STP to transport signaling among MSC and HLR.



**4. Operation Subsystem:** There are three areas of OSS, as shown in Fig.1.4. (1) network operation and maintenance functions, (2) subscription management, including charging and billing, and (3)mobile equipment management. These tasks require interaction between some or all of the infrastructure equipment. OSS is implemented in any existing network.

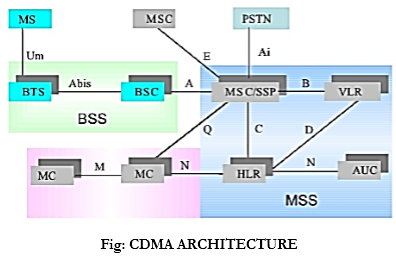
****

**Q2: Explain in details CDMA architecture with neat diagram.**

**Ans:-**

The code division multiple access (CDMA) system is a 2nd generation **digital mobile radio communication system** that provides for **voice and medium-speed data communication services**.

Upgrading to CDMA capability from 1st generation analog mobile systems allows CDMA service providers to add more customers for each radio tower (cell site), offer medium-speed data communication services, and to provide new high-value information services.



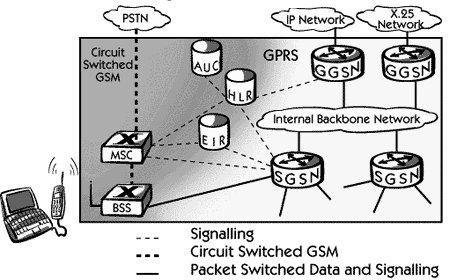
|  |  |
| --- | --- |
| BSS-Basic service set | manages radio interface b/w mobile stations and MSC consists of BTS and BSC. |
| MSC: Mobile switching center | It is a central unit equivalent to telephone exchange in a fixed network.  **Functions:**   1. Anchor MSC: Radio contact 2. Border MSC: Control BTS adjacent to location of mobile station HLR: maintains all subscriber related info and is responsible for managing mobile subscribers. Multiple MSCs are served by HLR |
| DMH: Data Message Handler | collecting billing data |
| OMC: Operation Maintenance center | overall management of wireless network |
| HLR: Home Location Register | Home subscriber information database |
| VLR: Visitor Location Register | linked to one or more MSCs. Dynamically stores subscriber information obtained from subscribers HLR data. During roaming MS enters a new service area covered by MSC. MSC informs associated VLR about the MS querying the HLR after MS goes through a registration process. |
| AUC: Authentication Center | manages Authentication |
| ELR: Equipment Identity Register | Provides information about mobile device for record purposes |
| MS: Mobile station | The MS may be a stand-alone piece of equipment for certain services or support the connection of external terminals, such as the interface for a personal computer or fax. |

**Q3:- Explain GPRS Architecture with neat diagram**

**Ans:-**

GPRS architecture works on the same procedure like GSM network, but, has additional entities that allow packet data transmission. This data network overlaps a second-generation GSM network providing packet data transport at the rates from 9.6 to 171 kbps. Along with the packet data transport the GSM network accommodates multiple users to share the same air interface resources concurrently.

Following is the GPRS Architecture diagram:



GPRS attempts to reuse the existing GSM network elements as much as possible, but to effectively build a packet-based mobile cellular network, some new network elements, interfaces, and protocols for handling packet traffic are required.

Therefore, GPRS requires modifications to numerous GSM network elements as summarized below:

|  |  |
| --- | --- |
| **GSM Network Element** | **Modification or Upgrade Required for GPRS.** |
| Mobile Station (MS) | New Mobile Station is required to access GPRS services. These new terminals will be backward compatible with GSM for voice calls. |
| BTS | A software upgrade is required in the existing Base Transceiver Station(BTS). |
| BSC | The Base Station Controller (BSC) requires a software upgrade and the installation of new hardware called the packet control unit (PCU). The PCU directs the data traffic to the GPRS network and can be a separate hardware element associated with the BSC. |
| GPRS Support Nodes (GSNs) | The deployment of GPRS requires the installation of new core network elements called the serving GPRS support node (SGSN) and gateway GPRS support node (GGSN). |
| Databases (HLR, VLR, etc.) | All the databases involved in the network will require software upgrades to handle the new call models and functions introduced by GPRS. |

## GPRS Mobile Stations

New Mobile Stations (MS) are required to use GPRS services because existing GSM phones do not handle the enhanced air interface or packet data. A variety of MS can exist, including a high-speed version of current phones to support high-speed data access, a new PDA device with an embedded GSM phone, and PC cards for laptop computers. These mobile stations are backward compatible for making voice calls using GSM.

## GPRS Base Station Subsystem

Each BSC requires the installation of one or more Packet Control Units (PCUs) and a software upgrade. The PCU provides a physical and logical data interface to the Base Station Subsystem (BSS) for packet data traffic. The BTS can also require a software upgrade but typically does not require hardware enhancements.

When either voice or data traffic is originated at the subscriber mobile, it is transported over the air interface to the BTS, and from the BTS to the BSC in the same way as a standard GSM call. However, at the output of the BSC, the traffic is separated; voice is sent to the Mobile Switching Center (MSC) per standard GSM, and data is sent to a new device called the SGSN via the PCU over a Frame Relay interface.

## GPRS Support Nodes

Following two new components, called Gateway GPRS Support Nodes (GSNs) and, Serving GPRS Support Node (SGSN) are added:

### **Gateway GPRS Support Node (GGSN)**

The Gateway GPRS Support Node acts as an interface and a router to external networks. It contains routing information for GPRS mobiles, which is used to tunnel packets through the IP based internal backbone to the correct Serving GPRS Support Node. The GGSN also collects charging information connected to the use of the external data networks and can act as a packet filter for incoming traffic.

### **Serving GPRS Support Node (SGSN)**

The Serving GPRS Support Node is responsible for authentication of GPRS mobiles, registration of mobiles in the network, mobility management, and collecting information on charging for the use of the air interface.

## Internal Backbone

The internal backbone is an IP based network used to carry packets between different GSNs. Tunneling is used between SGSNs and GGSNs, so the internal backbone does not need any information about domains outside the GPRS network. Signaling from a GSN to a MSC, HLR or EIR is done using SS7.

## Routing Area

GPRS introduces the concept of a Routing Area. This concept is similar to Location Area in GSM, except that it generally contains fewer cells. Because routing areas are smaller than location areas, less radio resources are used while broadcasting a page message.

|  |
| --- |
| **Second Answer of GPRS:-**   1. General Packet Radio Services is a new bearer service for GSM that greatly improves and simplifies wireless access to packet data networks. 2. GPRS applies packet radio principal to transfer user data packets in an efficient way between MS and external packet data network. 3. Modulation technique used in GPRS technology is GMSK. It is an important step on the path to 3G. It is a support to leading internet communication protocols. 4. GPRS uses radio channel i.e. 200 kHz wide. Radio channel carries digital data stream of 270.833 kbps. This rate is divided into 8 time slots each carrying 33.55 kbps per time slot. Data rate is 14.4 kbps per time slot and GPRS can combine upto 8 time slots giving data rate of 115 kbps. 5. The general packet radio service (GPRS) enhances GSM data services significantly by providing end-to-end packet switched data connections. This is particularly efficient in Internet/intranet traffic, where short bursts of intense datacommunications are actively interspersed with relatively long periods of inactivity. 6. As there is no real end-to-end connection to be established, setting up aGPRS call is almost instantaneous and users can be continuously on-line. 7. Usershave the additional benefits of paying for the actual data transmitted, rather thanfor connection time. 8. Because GPRS does not require any dedicated end-to-endconnection, it only uses network resources and bandwidth when data is actuallybeing transmitted. This means that a given amount of radio bandwidth can be shared efficiently among many users simultaneously. 9. Services of GPRS have been developed toreduce connection set-up time and allow an optimum usage of radio resources. 10. GPRS provides a packet data service for GSM where time slots on the air interfacecan be assigned to GPRS over which packet data from several mobile stations ismultiplexed. 11. GPRS is mainly used to send and receive data such as e-mail and web browsing. GPRS is relatively cheap service as compared to circuit switched data. 12. **GPRS terminals:**     1. Class A: MS supports simultaneous operation of GPRS and GPS services.     2. Class B: MS can able to register with the network for both GPRS and GSM services but can use only one of the two services at a given time.     3. Class C: MS can attach for either GPRS or GSM services.  * **Benefits of GPRS technology:**   1. Higher data rates (14.4-115 kbps)   2. Circuit switching and Packet switching can be used in parallel.   3. Constant connectivity   4. Easy billing   5. Efficient use of radio bandwidth. * **Limitations of GPRS technology:**   1. It has limited cell capacity.   2. Data rate is lower than mentioned   3. It does not provide store and forward service therefore if the MS is not available the data get lost. * **GPRS Architecture:** It is same as GSM architecture with some modifications as shown in figure. There is addition of new packet data switching and gatewaynodes, and an upgrade to existing nodes to provide a routing path for packetdata between the wireless terminal and a gateway node. The gateway node providesinterworking with external packet data networks for access to the Internet,intranet, and databases.   enter image description here  **A. Mobile station (MS):** Mobile station communicates with BSS by using radio air interface. To connect with SGSN the GPRS facility should be added in MS. It consists of User Equipment and SIM. SIM gives GM subscribers their identity . **B. Base Station Subsystem (BSS):** It consists of many BSC (Base Station Controller) and BTS (Base Transceiver Station). BSCs connect to single MSC and each BSC controls several hundred of BTSs. The BTS and BSC interface is called as Abis interface. BSC reduces burden on MSC in case of handover from one BTS to another connected to same BSC.  **C. Core Network (CN):**   1. **MSC (Mobile Switching Controller)** is the central unit of the network. It controls mobility management, call set up, location updating, routing, basic switching and supplementary services. 2. **HLR (Home Location Register)** consists of subscriber information and location of each user who reside in same city as MSC. It gives IMSI. 3. **VLR (Visitor Location Register)** temporarily stores the IMSI of each roaming subscriber. 4. **AUC (Authentication Centre)** is strongly protected database which handles authentication and encryption key for every single subscriber in HLR and VLR. It consists of EIR (Equipment Identity Register) to check for stolen phones. 5. It also consists of SGSN and GGSN.   **D. Serving GPRS Support Node (SGSN):** It is functionally connected with BSC and physically can be at MSC or BSC site. One SGSN can support BSCs of several MSC sites. Functions of SGSN are:   1. Authentication of GPRS mobiles. 2. Mobile registration in GPRS network. 3. Mobile mobility management. 4. Handling MO and MT traffic. 5. Collection of charging information of air interface usage 6. TCP/IP header compression   **E. Gateway GPRS Support Node**:   1. It interfaces GPRS backbone network and external packet data networks. 2. Converts the GPRS packets from SGSN to the PDP format 3. Converts PDP addresses to GSM addresses of the destination user. 4. It stores the current SGSN address and profile of the user in its location register. 5. There is many-to-many relation among SGSNs and GGSNs. |

**Q4:-Explain in detail EDGE Network Architecture with neat diagram.**

**Ans:-**

EDGE is an evolution to the GSM mobile cellular phone system. The name EDGE stands for Enhanced Data rates for GSM Evolution and it enables data to be sent over a GSM TDMA system at speeds up to 384 kbps. This means it offers a significantly higher data rate than GPRS.

**There are a number of key elements in the upgrade from GSM or GPRS to EDGE. The GSM EDGE technology requires a number of new elements to be added to the system:**

1. **Use of 8PSK modulation:**   In order to achieve the higher data rates within GSM EDGE, the modulation format can be changed from GMSK to 8PSK. This provides a significant advantage in being able to convey 3 bits per symbol, thereby increasing the maximum data rate. This upgrade requires a change to the base station. Sometimes hardware upgrades may be required, although it is often simply a software change.
2. **Base station:**   Apart from the upgrade to incorporate the 8PSK modulation capability, other small changes are required to the base station. These are normally relatively small and can often be accomplished by software upgrades.
3. **Upgrade to network architecture:**   GSM EDGE provides the capability for IP based data transfer. As a result, additional network elements are required.   
     
   The two main additional nodes required for the network are the Gateway GPRS Service Node (GGSN) and the Serving GPRS Service Node (SGSN).
   1. The GGSN connects to packet-switched networks such as the Internet and other GPRS networks.
   2. The SGSN provides the packet-switched link to mobile stations.
4. **Mobile stations*:***   It is necessary to have a GSM EDGE handset that is EDGE compatible. As it is not possible to upgrade handsets, this means that the user needs to buy a new GSM EDGE handset.

## GSM EDGE network architecture upgrades:-

## The main new network architecture entities that are needed for the EDGE upgrade are:

1. **SGSN:**   GPRS Support Node - this forms a gateway to the services within the network.

The SGSN or Serving GPRS Support Node element of the GPRS network provides a number of takes focused on the IP elements of the overall system. It provides a variety of services to the mobiles:

1. Packet routing and transfer
2. Mobility management
3. Authentication
4. Attach/detach
5. Logical link management
6. Charging data

There is a location register within the SGSN and this stores location information (e.g., current cell, current VLR). It also stores the user profiles (e.g., IMSI, packet addresses used) for all the GPRS users registered with the particular SGSN.

**2. GGSN:**   Gateway GPRS Support Node which forms the gateway to the outside world.

The GGSN, Gateway GPRS Support Node is one of the most important entities within the GSM EDGE network architecture.

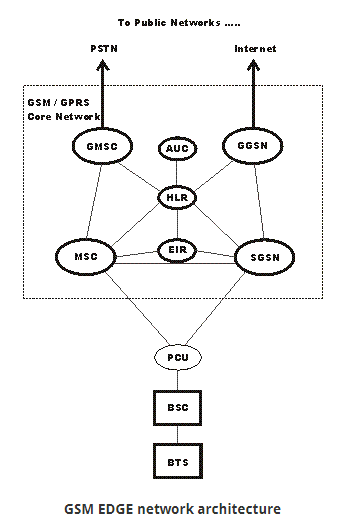
The GGSN organizes the inter-working between the GPRS / EDGE network and external packet switched networks to which the mobiles may be connected. These may include both Internet and X.25 networks.

The GGSN can be considered to be a combination of a gateway, router and firewall as it hides the internal network to the outside. In operation, when the GGSN receives data addressed to a specific user, it checks if the user is active, then forwarding the data. In the opposite direction, packet data from the mobile is routed to the right destination network by the GGSN.

**3. PCU:**   Packet Control Unit which differentiates whether data is to be routed to the packet switched or circuit switched networks.

The PCU or Packet Control Unit is a hardware router that is added to the BSC. It differentiates data destined for the standard GSM network (circuit switched data) and data destined for the EDGE network (Packet Switched Data). The PCU itself may be a separate physical entity, or more often these days it is incorporated into the base station controller, BSC, thereby saving additional hardware costs.

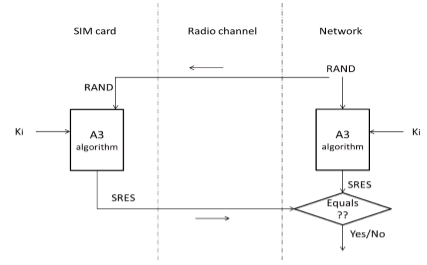
A simplified view of the GSM EDGE network architecture can be seen in the diagram below. From this it can be seen that it is very similar to the more basic GSM network architecture, but with additional elements.

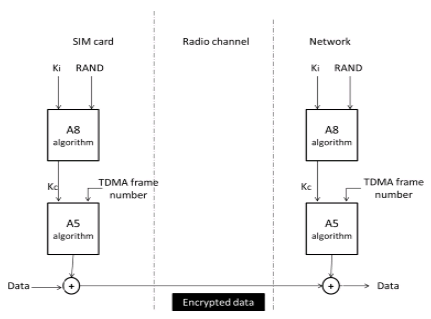
****

**Q5: Explain in detail GSM Privacy and Authentication with neat diagram**

**Ans:-**

1. The data being transmitted via GSM is in digital form and hence is much easier to carry out digital transformation, data encryption, scrambling and protection methods against unauthorized access to transmitted information to support privacy
2. system needs to verify before connecting two terminals if the connection has been tapped or compromised and that the authorized user is at both the ends of connection i.e. Authentication.
3. Various security measures are implemented in GSM transmission like:
   1. Provide access to the network only after user authenticity’s verification.
   2. Encrypt the transmitted data.
   3. Usage of temporary mobile user identity number (e.g. TMSI)
4. Three algorithms have been specified for security services in GSM networks.
   1. Algorithm A3 → Authentication
   2. Algorithm A5 → Encryption
   3. Algorithm A8 → Generation of Cipher Key
5. **Subscriber Identity Module (SIM):**
   1. The SIM card as it is popularly called is a microcontroller embedded plastic card is an important element ensuring security in GSM system.
   2. The SIM card is placed inside the Mobile device in the compartment allocated for it. Every Network operator provides his own SIM card during registration of phone.
   3. It is the main identity of user on a Cellular network. Since it is portable, we can also use a single card on multiple devices.
   4. Network operators also provide SIM replacement in case of theft of device or damage. Security service (e.g. Police Cyber Cell) tracks stolen phones from SIM data.
   5. A SIM card contains ROM, RAM and a NVM (Non-volatile memory)
   6. ROM contains the program for A3 and A8 algorithms in it.
   7. RAM is used for processing and storing real-time data.
   8. **NVM is used for storing individual user’s parameters and data. The various parameter’s and data in NVM are :**
      1. Ki →The user’s authentication key
      2. IMSI → International Mobile Subscriber Identity which is made up of Country code, network code and user’s number.
      3. TMSI → Temporary Mobile Subscriber Identity which is generated after a user register’s in a new VLR.
      4. LAI → Location Area Identifier.
      5. Personal Phone-book.
      6. Received SMS
      7. PIN → Personal Identification Number which identifies user with respect to the SIM card.
6. **Authentication Process:**
   1. The mobile network sends a pseudorandom number RAND (as seen in the figure below) to the Mobile Station(MS i.e. the user’s Cell phone)
   2. Now at the MS, a 32-bit electronic signature known as SRES is derived using the RAND received from the network.
   3. At the same time, the mobile network also calculates the SRES using the same RAND that it provided to the MS.
   4. Now the SRES calculated at the MS is sent to the network and compared.
   5. If both are identical, then the authentication is complete.



1. **Encryption Process:**
   1. The encryption process is achieved by the use of A5 algorithm. The security of this algorithm lies in the fact that the key is never transmitted over the air.
   2. The A5 algorithm is realized inside the mobile phone.
   3. The SIM card initially calculates the encryption-key Kc based on the key Ki and the RAND number received during authentication process.
   4. Now the using the Kc and the current 22-bit TDMA frame number, the A5 algorithm generates a 114-bit number.
   5. It is then modulo-2 added to the information bits (i.e. data) of the normal burst. This is the encrypted data. It’s then transmitted.
   6. Similarly, on the network operator’s side, the same process as above is carried out and final 114-bit number is generated.
   7. If the encrypted data and the 114-bit number generated by the operator is modulo-2 added, we get original data.
2. 

**Q6: Compare CDMA 2000 & WCDMA**

Ans:-

|  |  |  |
| --- | --- | --- |
|  | WCDMA | Cdma2000 |
|  | 3G technology evolved from GSM technology | 3G technology evolved from IS-95 CDMA technique |
| Carrier Spacing : spacing between CDMA operators to obtain channel protection | 5 MHz | 3.75 MHz |
| Chip Rate : number of DSSS pulses per second; a chip is a pulse of DSSS code | 4.096 MHz | 3.68 MHz |
| Spreading Factor : SF=(Chip Rate)/(Data Rate) | Higher | Lower |
| Power Control Frequency : the output power of the transmitter is controlled by itself at this frequency | 1500 Hz | 800 Hz |
| Frame Duration : the time duration of a frame;between beginning and end of the frame. | 10 ms | 20 ms (also uses 5, 30, 40 ms frames) |
| Base Stations : base stations may or may not need synchronous timings | Asynchronous | Synchronous |
| Forward Link Pilot : The pilot is a channel modulated only by the PN (Pseudo Noise) spreading codes | TDM, Dedicated pilot | CDM, Common Pilot |
| Antenna Beam Forming : used for directional signal transmission & reception | TDM, Dedicated pilot | Auxiliary pilot |
| Modes of operation | FDD and TDD | FDD |
| Overhead | High (because of non-shared,pilot code Channel) | Low (because of shared pilot,code Channel) |
| Core network | GSM MAP | ANSI-41 MAP |

**Q7: Write short note on Handoff Strategies**

### Ans:-

### **Handoff:-**

### When a mobile moves into a different cell while a conversation is in progress, the MSC automatically transfers the call to a new channel belonging to the new base station. This handoff operation not only involves identifying a new base station, but also requires that the voice and control signals be allocated to channels associated with the new base station.

**Handoff Strategies:-**

### In order to meet handoff strategies requirements, system designers must specify an optimum signal level at which to initiate a handoff. Once a particular signal level is specified as the minimum usable signal for acceptable voice quality at the base station receiver (normally taken as between –90 dBm and –100 dBm), a slightly stronger signal level is used as a threshold at which a handoff is made. This margin, given by Δ = Pr handoff – Pr minimum usable, cannot be too large or too small. If Δ is too large, unnecessary handoffs which burden the MSC may occur, and if Δ is too small, there may be insufficient time to complete a handoff before a call is lost due to weak signal conditions. Therefore, Δ is chosen carefully to meet these conflicting requirements. Figure  illustrates a handoff situation.

### In first generation analog cellular systems, signal strength measurements are made by the base stations and supervised by the MSC. Each base station constantly monitors the signal strengths of all of its reverse voice channels to determine the relative location of each mobile user with respect to the base station tower. In addition to measuring the RSSI of calls in progress within the cell, a spare receiver in each base station, called the locator receiver, is used to scan and determine signal strengths of mobile users which are in neighboring cells. The locator receiver is controlled by the MSC and is used to monitor the signal strength of users in neighboring cells which appear to be in need of handoff and reports all RSSI values to the MSC. Based on the locator receiver signal strength information from each base station, the MSC decides if a handoff is necessary or not.

### In second generation systems, handoff decisions are mobile assisted. In mobile assisted handoff (MAHO), every mobile station measures the received power from surrounding base stations and continually reports the results of these measurements to the serving base station. A handoff is initiated when the power received from the base station of a neighboring cell begins to exceed the power received from the current base station by a certain level or for a certain period of time. The MAHO method enables the call to be handed over between base stations at a much faster rate than in first generation analog systems since the handoff measurements are made by each mobile, and the MSC no longer constantly monitors signal strengths. MAHO is particularly suited for microcellular environments where handoffs are more frequent.

**Types of Handoff**

1. Hard handoff:-

- A hard handoff is essentially a “break before make” connection. In hard handoff, the link to the prior base station is terminated before or as the user is transferred to the new cell’s base station, this means that the mobile station is **linked to no more than one base station at a given time**. Under the control of the MSC, the BS hands off the MS’s call to another cell and then drop the call. Hard handovers are intended to be instantaneous in order to minimize the disruption to the call. Initiation of the handoff may begin when the signal strength at the mobile received from base station 2 is greater than that of base station.

**Types of Hard Handover:**

There are two types of hard handover:-

**i) Inter-cell Handover**: The most basic form of handover is when a phone is redirected from its current cell (source) to a new cell, while call in progress. In terrestrial networks, the source and the target cells may be served from two different cell sites or from one and the same cell site. This type of handover, in which the source and the target are different cells (even if they are on the same cell site), is called inter-cell handover. So the purpose of inter-cell handover is to maintain the call as the subscriber is moving out of the area covered by the source cell and entering the area of the target cell.

**ii) Intra-cell Handover**: In this handover, the source and the target are one and the cell is same and only the used channel is changed during the handover. So in this handover, in which the cell is not changed, is called intra-cell handover and the purpose of intra-cell handover is to change one channel, which may be faded or interfered with a new clearer or less fading channel.

**iii) Microcellular Handover**: This handover technique is mostly used to meet high system capacity by reuse of frequency and is mostly used in populated areas. Fig.3 shows that there are three Base Stations in three streets. There is a line of sight (LOS) between BS1 and BS3 where as there is no line of sight (NLOS) between BS2 and BS1. Therefore we can say that there is LOS handover between BS1 and BS3 whereas between BS2 and BS1 there is NLOS handover.

2. **Soft Handoff:**

Soft handoff (or handover) is a mobile cellular network technology commonly used in CDMA (Code-division multiple access) systems that enables the overlapping of the repeater coverage zones, so that every mobile station is always well within range of at least one of the base stations.

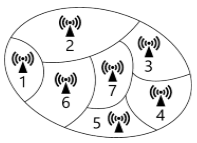
**A Soft handoff mechanism works by first switching and establishing connection with another base station before** **disconnecting from the existing base station in the network**, so it is also sometimes referred to as “Make-before- Break” Handoff.

In comparison to hard handoff, technical implementation of a Soft handoff is more expensive and complex. Now the soft handoff procedure is as follows: Suppose that the mobile station is linked and communicating with base station 1. Every base station is sending a pilot signal, which among other things, gives a measure of the signal strength to mobile users. When the signal strength of base station 2 exceeds the add threshold, base station 1 is notified to place base station 2 onto the candidate list. Further, when the signal strength of base station 2 becomes greater than that of base station 1 by some specified level, Base station 2 is placed on the active list and it also is allowed control of the call. Here, diversity combining is implemented. Now upon the signal level of base station 1 going below the drop threshold, the drop timer is activated. If it happens now that the signal level of base station 1 goes back above the drop level, the drop timer will be reset. However, if the signal strength level goes below the drop threshold and the drop timer expires; base station1 is dropped from activity with the call.

**Other Information:-**

|  |  |
| --- | --- |
| GSM handoff | CDMA handoff |
| **Intra-cell handover:**  **Inter-cell handover**  **Inter-BSC handover**  **Inter-MSC handover:** | Soft  Softer  Hard  idle |
| Note: refer text book for more details |  |

## Q8: Consider a simple high power transmitter that can support 100 voice channel s covering given a service area. Let the service area be divided into seven smaller area cells. As shown in figure, each supported by lower power transmitters. The available spectrum of 100 voice channels is divided into 4 groups of 25 channels each. The cells (1,7)(2,4)(3,5) and six are assigned distinct channel groups. Show that the total no of channels that can be supported is enhanced to 175 to cover the same service area.



Total no of Channels available, N=100

**Case 1:** A single high power transmission transmitter is used to cover the given service area

This implies that it is a non-cellular system

Therefore, No of channels in system are limited to 100 only.

**Case 2:** Service area is divided into seven cells.

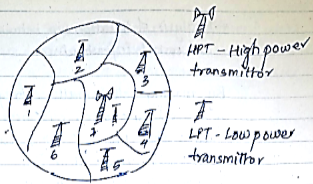
No. of distinct cells = 7

No. of channel groups = 4.

No. of channels per channel group =25

Step1: Allocation of channel groups to cells

Let channel group I be allocated to cells 1 as well as 7, channel group 2 be allocated to cells 2 as well as 4; channel group 3 be allocated to cells 3 as well as 5 and channel group 4 be allocated to cell 6 as shown in figure



Step2: Total no of channels available in the specified cellular system

Total no. of channels allocated to all cells is equal to no. of channels per channel group multiplied by the Number of distinct cells i.e.

Total no. of channels allocated to all cells = 25\*7

Hence, total no. of channels available=175 channels

Total no. of channels that can be supported by given cellular system is increased to 175 from 100 in a Non-cellular system to cover the same service area.

### **Q9:- Consider a cellular network with 64 cells. Each hexagonal cell has an appropriate area of 10Km2. Total no of radio channels allotted for the network is 336. Find the total number of channels of the network, if**

### **a) N = 4**

### **b) N = 7**

### **c) N =12, where N denotes cell reuse**

Ans:-

Total number of cells = 64. Each cell area = 10 km2.

The total area covered by the cellular network is, 64 X 10 = 640 km2.

It is given that the total available channels in the network = 336.

1. (a) For N = 4, the available channels in a cell = 336/4 = 84
   1. Total channels = 84 X 64 = 5,376 channels.
2. (b) For N = 7, the available channels in a cell = 336/7 = 48
   1. Total channels = 48 X 64 = 3,072 channels.
3. (c) For N = 12, the available channels in a cell = 336/12 = 28
   1. Total channels = 28 X 64 = 1,792 channels.

**Q10:-Problem on cellular network design**

**Q11 Problem on cellular network design**

**3: Wireless in Local Loop**

Q1: Write short note on MMDS

Q2: Explain in detail MMDS and LMDS working in WLL based technology.

Q3: Write short note on WLL Architecture.

Q4: Neatly explain the WLL Architecture. Explain the two local loop techniques with diagram

Ans:-

**Wired Local Loop:** . In telephone, loop is a circuit line from a subscriber’s phone to a line-terminating equipment at a central office. In traditional telephone networks, your phone would be connected to the nearest exchange through a pair of copper wires.

**Wireless Local Loop (WLL):**

1. Implementation of a local loop especially in rural areas or geographically placed remote areas used to remain a risk for many operators due to less users and increased cost of materials. The loop lines are copper wires which require more investments.Wireless local loop (WLL) technology simply means that the subscriber is connected to the nearest exchange through a radio link instead of through these copper wires.

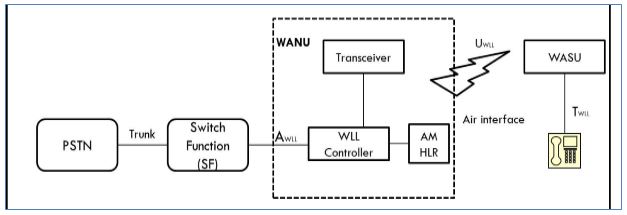
2. However today with Wireless local loop (WLL) has been introduced which solves most of these problems.

3. As WLL is wireless, the labor-charges and time-consuming investments are no longer relevant.

4. WLL systems can be based on one of the four below technologies:

1. Satellite-based systems.
2. Cellular-based systems.
3. Microcellular-based Systems
4. Fixed Wireless Access Systems

**5. The WLL architecture is shown below:**



6. The architecture consists of three major components i.e WANU, WASU and SF

**7. Wireless Access network unit (WANU): the WANU consists of various components which include**

1. several base stations transceivers or radio ports (RP)
2. a Radio port control unit
3. an Access manager (AM)
4. an HLR.

**8. It provides various functionalities like:**

1. Authentication
2. Air interface privacy
3. Over-the-air registration of subscriber units.
4. Operations and Maintenance
5. Routing
6. Billing
7. Switching functions
8. Transcoding of voice and data.

9. Wireless access subscriber unit (WASU): It provides an air interface UWLL towards the network and a traditional interface TWLL towards the subscriber.

10 The power supply for it is provided locally.

**11 The interface includes**

1. protocol conversion and transcoding
2. authentication functions
3. signaling functions

12 The TWLL interface can be an RJ-11 or RJ-45 port.

13 The UWLL interface can be AMPS, GSM, DECT and so one.

14 Switching Function (SF): The switching function (SF) is associated with a switch that can be digital switch with or without Advanced Intelligent Network (AIN) capability, an ISDN switch or a Mobile Switching Centre (MSC).

15 The AWLL interface between the WANU and the SF can be ISDN-BRI or IS-634 or IS-653 or such variants.

**Deployment Issues:**

16. To compete with other local loop technologies WLL needs tom [provide sufficient coverage and capacity, high circuit quality and efficient data services.

17. Moreover the WLL cost should be competitive with its wire line counterpart.

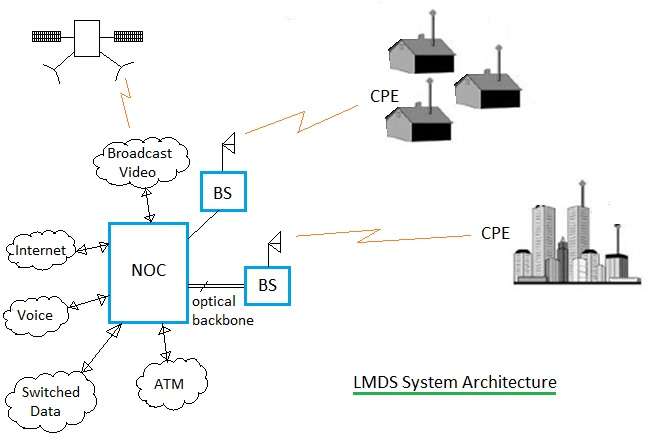
18. **Various issues are considered in WLL development which include**:

1. **Spectrum:** The implementation of WLL should be flexible to accommodate different flexible bands as well as non-continuous bands. More these bands are licensed by government.
2. **Service quality:** Customer expects that the quality of service should be better than the wireline counterpart. The quality requirements include link quality, reliability and fraud immunity.
3. **Network Planning:** Unlike Mobile System, WLL assumes that user is stationary, not moving. Also the network penetration should be greater than 90%. Therefore WLL should be installed based on parameters like Population Density etc.
4. **Economics:** Major cost here is electronic equipment’s. In current scenario, the cost of such electronic equipment is reducing periodically.

**LMDS and MMDS**

**Both LMDS and MMDS are Broadband WLL (Wireless Local Loop) technologies** developed as alternative to DSL wireless technologies such as ADSL, VDSL etc. **These technologies are used for video, voice, ATM and internet applications.**

### **LMDS Architecture**

  
**Fig-1: LMDS Architecture**

LMDS is the short form of Local Multipoint Distribution Service. It is a P2MP (Point to Multi-Point) technology operating above 20 GHz. P2P (Point to Point) and TV systems can also be interfaced with LMDS.

The figure-1 depicts LMDS architecture. It consists of NOC (Network Operation Center), BS (Base Station), CPE (Customer Premises Equipment), fiber based infrastructure. Multiple NOCs are interconnected together. Fiber backbone infrastructure consists of SONET, OC-12, OC-3, DS3 optical links, CO equipment’s etc. Moreover NOC is interfaced with ATM, IP systems, PSTN and Internet.

BS is interfaced with optical equipment’s on one side and wireless on the other. It houses optical to electrical and electrical to optical interfaces as well as RF up/down converters. RF up converter is used to convert data to be transmitted on modulated RF waveforms. The RF down converter does the reverse operation.

CPEs are installed at customer premises and are linked with BS using wireless microwave links. They are available from multiple vendors. It consists of functionalities viz. modulation, demodulation, RF up conversion and RF down conversion etc. CPEs utilize multiple access schemes viz. TDMA, FDMA and CDMA for communication with BSs in the LMDS network.

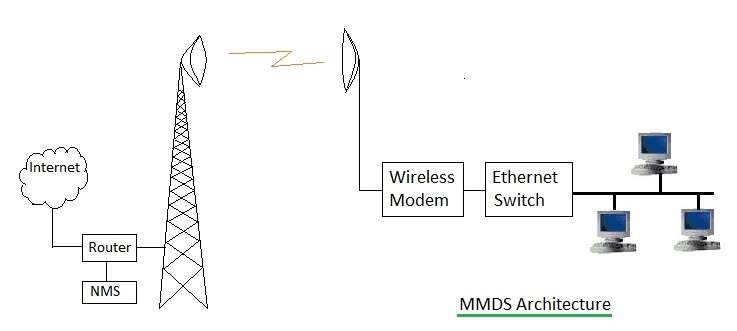
**Following are the key features of LMDS system**:   
 1 It operates at 28 GHz or 38 GHz frequency.   
 2 It is installed similar to cellular system cell based layout.   
 3 Cell size or range of BS is 5 miles.   
 4 It uses P2MP and P2P topologies for end communication with CPEs.

### **LMDS Advantages and Disadvantages**

1. Following are the LMDS advantages:   
   1 It has larger bandwidth used for wide variety of applications such as voice, IP, data etc.   
   2 It supports large capacity of users densely populated by way of sectorizing the area into cells.
2. Following are the LMDS disadvantages:   
   1 It has high RF equipment costs due to larger number needed.   
   2 Smaller cell size (i.e. 2 to 8 Km) due to requirement of covering large capacity of users.   
   3 Requires many cells to cover larger city areas. This increases installation cost for service providers.

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

### **MMDS Architecture**

  
Fig-2: MMDS Architecture 

MMDS is the short form of Multichannel Multipoint Distribution Service. It is used for small business and home offices. It is not used for large customer requirements such as central offices. It is used where other broadband wireless technologies are difficult to be installed. It uses microwave tower installed on top of the mountains or tall buildings. It covers larger distance compare to LMDS which is about 35 miles.

The figure-2 depicts MMDS architecture. It consists of Hub equipment and customer side equipments. Hub consists of antenna tower, RF equipment, Modem, Router for connection with internet and network management system (i.e. NMS). Customer side equipment include antenna, wireless modem, ethernet switch, PCs etc. Hub antenna tower receives wireless signals from multiple users similar to P2MP topology. Each user premise antenna and Hub antenna is connected with P2P microwave link.

**Following are the key features of MMDS system:**

1. It operates in 2.5 GHz and 3.5 GHz frequency bands.   
2.  Hub tower has coverage distance of about 35 miles.   
3. It uses both P2MP and P2P topologies. P2MP from multiple users to Hub and P2P between individual user and Hub.

### **MMDS Advantages and Disadvantages**

1. Following are the MMDS advantages:   
   1 The RF propagation covers 100 Km of region using single antenna tower.   
   2 Due to smaller frequency of use compare to LMDS, MMDS does not suffer from rain attenuation.   
   3 RF equipment’s are cheaper at lower frequency of 2.5GHz or 3.5 GHz and are available in large quantities.
2. Following are the MMDS disadvantages:   
   1 It does not support larger capacity due to lack of sectorization concept in MMDS.   
   2 It suffers from interference from other MMDS and TV applications.   
   3 Large upstream bandwidth needs more and accurate planning.

**4: Wireless Local Area Network**

**Q1: Write short note on WLAN Architecture.**

**Or Explain in detail IEEE 802.11 WLAN Architecture**

**Ans:-**

1. "Wireless LAN", also referred Radio LAN (WLAN) if the communication medium is the radio (not light infrared for example).

2. The stations of the wireless network can communicate directly with each other, we called Ad Hoc network type, or via relay terminals called APs (Access Points, PA) then it is an infrastructure network.

**3. There are two types of wireless networks:**

i)Ad Hoc, where stations communicate directly;  
ii) Infrastructure type networks where stations communicate through access points.

4. To communicate, each station must of course be equipped with an adapter WiFi and a radio antenna.

5. The 802.11architecture defines two types of services and three different types of stations

## 802.11 Services

The two types of services are

1. Basic services set (BSS)

2. Extended Service Set (ESS)

**1. Basic Services Set (BSS)**

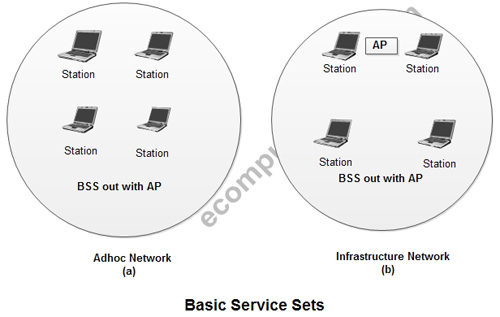
a) The basic services set contain stationary or mobile wireless stations and a central base station called access point (AP).

b) The use of access point is optional.

c) If the access point is not present, it is known as stand-alone network. Such a

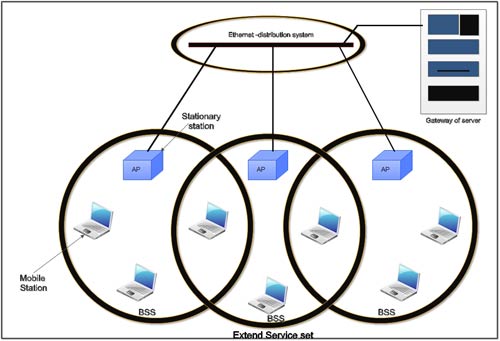
BSS cannot send data to other BSSs. This type of architecture is known as adhoc architecture.

d) The BSS in which an access point is present is known as an infrastructure network.

[](http://ecomputernotes.com/images/Basic-Service-Sets.jpg)

**2. Extend Service Set (ESS)**

a) An extended service set is created by joining two or more basic service sets (BSS) having access points (APs).

[](http://ecomputernotes.com/images/Extend-Service-Set.jpg)

b) These extended networks are created by joining the access points of basic services sets through a wired LAN known as distribution system.

c) The distribution system can be any IEET LAN.

d) There are two types of stations in ESS:

(i) **Mobile stations**: These are normal stations inside a BSS.

(ii) **Stationary stations**: These are AP stations that are part of a wired LAN.

e) Communication between two stations in two different BSS usually occurs via two APs.

f) A mobile station can belong to more than one BSS at the same time.

## ****802.11 Station Types****

IEEE 802.11 defines three types of stations on the basis of their mobility in wireless LAN. These are:

1. No-transition Mobility

2. BSS-transition Mobility

3. ESS-transition Mobility

1. **No-transition .Mobility**: These types of stations are either stationary *i.e.*immovable or move only inside a BSS.

2. **BSS-transition mobility**: These types of stations can move from one BSS to another but the movement is limited inside an ESS.

3. **ESS-transition mobility**: These types of stations can move from one ESS to another. The communication mayor may not be continuous when a station moves from one ESS to another ESS.

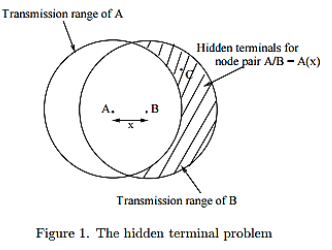
Q2: Explain in detail Hidden and Exposed terminal problem with respect to WLAN.

Ans:-

Communication among nodes using radios are called WLAN where every device can communicate to its direct neighbors,

**Hidden terminal problem:- .**

1. Suppose that node A wants to transmit to node B located at a distance x from A. By only sensing the medium, node A will not be able to hear transmissions by any node (C) in the dashed area denoted by A(x), and will start transmitting, leading to collisions at node B. This is the well-known hidden terminal problem, where the hidden nodes are located in the area A(x).



2. RTS/CTS handshake mechanism was introduced to wireless MAC layers to eliminate the hidden terminal problem. However, this mechanism introduces a new problem termed the exposed terminal problem. We assume here an RTS/CTS exchange so that the issue of hidden terminal is addressed.

**Exposed Terminal Problem:-**

Let us consider Figure 2 and assume that node A wants to transmit to node B.



1. Node A sends an RTS and waits for B to send a CTS. Suppose a node D located in area Y (x) wants to transmit data to node C located in area X(x), and D transmits a RTS to C just before A sends the RTS to B. After receiving the RTS from D, C transmits a CTS. This CTS is heard by B upon which B will enter a back off period preventing B from sending the CTS to A.

2. Therefore, any transmission from a node within the area Y to a node within X(x) will prevent A from transmitting data to B, although simultaneous transmissions from area Y (x) to X(x) would not have interfered with transmission from A to B. We define the terminals in the region Y (x) as the exposed terminals for the node pair A/B. In this case, the number of transmissions that could occur between nodes from area X(x) and nodes from area Y (x) can be expressed as XY .

**Q3: Explain in detail the IEEE 802.11 Mac layer.**

**Ans:-**

## ****MAC sublayer Functions****

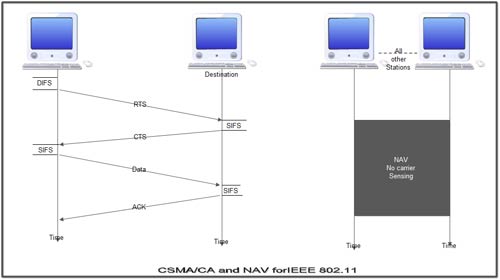
802.11 support two different modes of operations. These are:

1. Distributed Coordination Function (DCF)

2. Point Coordination Function (PCF)

**1. Distributed Coordination Function**

* 1. The DCF is used in BSS having no access point.
  2. DCF uses CSMA/CA [protocol](http://ecomputernotes.com/computernetworkingnotes/computer-network/protocol) for transmission.
  3. The following steps are followed in this method.

[](http://ecomputernotes.com/images/CSMA-CA-and-NAV-for-IEEE-802.11.jpg)

1. When a station wants to transmit, it senses the channel to see whether it is free or not.

2. If the channel is not free the station waits for back off time.

3. If the station finds a channel to be idle, the station waits for a period of time called distributed interframe space (DIFS).

4. The station then sends control frame called request to send (RTS) as shown in figure.

5. The destination station receives the frame and waits for a short period of time called short interframe space (SIFS).

6. The destination station then sends a control frame called clear to send (CTS) to the source station. This frame indicates that the destination station is ready to receive data.

7. The sender then waits for SIFS time and sends data.

8. The destination waits for SIFS time and sends acknowledgement for the received frame.

## ****Collision avoidance****

* 1. 802.11 standard uses Network Allocation Vector (NAV) for collision avoidance.
  2. The procedure used in NAV is explained below:

1. Whenever a station sends an RTS frame, it includes the duration of time for which the station will occupy the channel.

2. All other stations that are affected by the transmission creates a timer caned network allocation vector (NAV).

3. This NAV (created by other stations) specifies for how much time these stations must not check the channel.

4. Each station before sensing the channel, check its NAV to see if has expired or not.

5. If its NA V has expired, the station can send data, otherwise it has to wait.

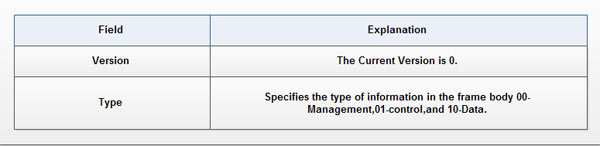
## ****2. Point Coordination Function****

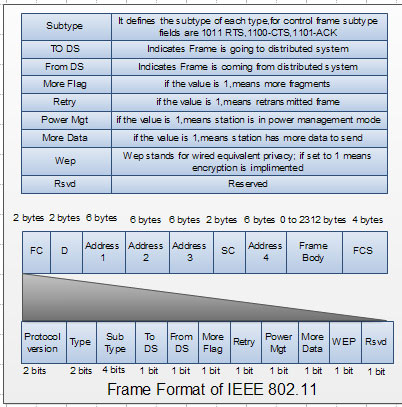
* 1. PCF method is used in infrastructure network. In this Access point is used to control the network activity.
  2. It is implemented on top of the DCF and IS used for time sensitive transmissions.
  3. PCF uses centralized, contention free polling access method.
  4. The AP performs polling for stations that wants to transmit data. The various stations are polled one after the other.
  5. To give priority to PCF over DCF, another interframe space called PIFS is defined. PIFS (PCF IFS) is shorter than DIFS.
  6. If at the same time, a station is using DCF and AP is using PCF, then AP is given priority over the station.
  7. Due to this priority of PCF over DCF, stations that only use DCF may not gain access to the channel.
  8. To overcome this problem, a repetition interval is defined that is repeated continuously. This repetition interval starts with a special control frame called beacon frame.
  9. When a station hears beacon frame, it start their NAV for the duration of the period of the repetition interval.

## Frame Format ****of 802.11****

The MAC layer frame consists of nine fields.

**1. Frame Control**(FC). This is 2 byte field and defines the type of frame and some control information. This field contains several different subfields.

These are listed in the table below:                                 [](http://ecomputernotes.com/images/Frame-Format-802.11.jpg)

[](http://ecomputernotes.com/images/Frame-Format-of-IEEE-802.11.jpg)

2.**D**. It stands for duration and is of 2 bytes. This field defines the duration for which the frame and its acknowledgement will occupy the channel. It is also used to set the value of NA V for other stations.

3. **Addresses**. There are 4 address fields of 6 bytes length. These four addresses represent source, destination, source base station and destination base station.

4. **Sequence Control (SC).** This 2 byte field defines the sequence number of frame to be used in flow control.

5. **Frame body**. This field can be between 0 and 2312 bytes. It contains the information.

6. FCS. This field is 4 bytes long and contains 'cRC-32 error detection sequence.

**IEEE 802.11 Frame types**

There are three different types of frames:

1. Management frame

2. Control frame

3. Data frame

1. **Management frame**. These are used for initial communication between stations and access points.

2. **Control frame**. These are used for accessing the channel and acknowledging frames. The control frames are RTS and CTS.

3. **Data frame**. These are used for carrying data and control information.

## 802.11 Addressing

• There are four different addressing cases depending upon the value of *To DS And from*DS subfields of FC field.

• Each flag can be 0 or 1, resulting in 4 different situations.

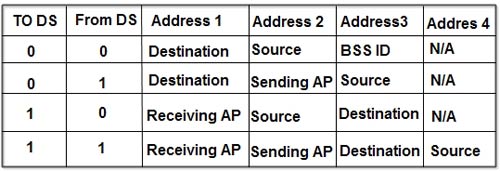
1. If *To*DS = 0 and *From*DS = 0, it indicates that frame is not going to distribution system and is not coming from a distribution system. The frame is going from one station in a BSS to another.

2. If *To*DS = 0 and *From*DS = 1, it indicates that the frame is coming from a distribution system. The frame is coming from an AP and is going to a station. The address 3 contains original sender of the frame (in another BSS).

3. If *To*DS = 1 and *From*DS = 0, it indicates that the frame is going to a distribution system. The frame is going from a station to an AP. The address 3 field contains the final destination of the frame.

4. If *To*DS = 1 and *From*DS = 1,it indicates that frame is going from one AP to another AP in a wireless distributed system.

The table below specifies the addresses of all four cases.

[](http://ecomputernotes.com/images/Addresses-of-all-four-cases.jpg)

**Q4: Explain in detail wireless security offered by IEEE 802.11 in detail with neat diagram.**

**Ans:-**

WLAN Security Technologies There are several security technologies introduced to solve the authentication problem and to preserve the privacy and integrity of data transmitted on air. IEEE802.11 specified three basic security technologies to authenticate access to the WLAN and to preserve the privacy of data transmitted:-

**1. open system authentication,**

**In the open-system** method all communications between the STA and the AP are in the clear (i.e. visible and not hidden). In this method it does not matter if the WEP keys used to access the WLAN are correct, the AP will allow accessing the WLAN even if the keys used are invalid, the only requirement here is the network SSID . However, APs broadcast their SSID by default so using open-system authentication is totally insecure.

**2. shared key authentication**

In the shared key method, the AP sends a challenge text to the STA; this challenge is encrypted by WEP keys then it is returned back to the AP to either grant access to the WLAN or not. The AP will decrypt the received challenge and compare it with the original challenge it stores. If the decrypted challenge found identical to the original challenge then it implies that the AP and the STA are using the same WEP key; hence the STA can be authenticated. In this scenario, the authentication of STAs is mandatory while AP authentication is not important .This means that a legitimate STA can connect to an illicit AP. Another problem in shared authentication scheme is that an attacker can sniff the data traffic, especially the challenge text and the encrypted response to the challenge, doing that, it will be possible to find out the secret encryption keys and as result infringing the security of the network. Unfortunately the default authentication method in most APs is the open-system method.

**3.**

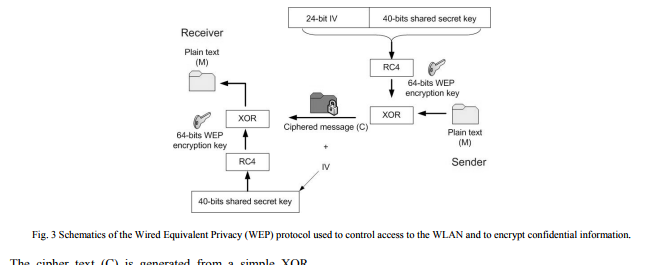
Another authentication technique also used is based on the STA MAC address information. Accessing the WLAN can be filtered on the bases of STA's MAC addresses. This means that all authorized STA's MAC addresses have to be listed in a lookup table stored in the AP or a network connected Authentication server. Only STAs which their MAC addresses listed in the table will be able to access the WLAN. The problem in this technique is the ease of data traffic monitoring hence it becomes trivial to capture the MAC address of an authenticated wireless station. Doing that and with the help of some publicly available tools, an attacker can spoof the AP by using an authenticated MAC address and breach the security of the WLAN. This does not mean that such technique can never be used, in fact it can be used in some special situations but it is not recommended in public WLANs. Some researchers tried to develop new techniques to discover attacks using false or spoofed MAC addresses

**4 WEP :-**

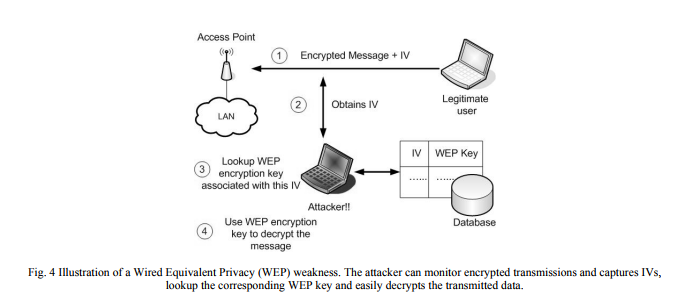
Wired Equivalent Privacy (WEP): WEP is the security protocol in use since the early IEEE802.11 standard . It is used to secure communications between APs and STAs and to provide secured authentication schemes; the aim was to provide security to the WLAN similar to the security provided in the wired LAN. It is based on a stream cipher encryption algorithm called "RC4". WEP is used to control access to the WLAN and to encrypt confidential information. It was proved theoretically and practically that WEP failed as a security protocol because of many problems. To access a WLAN in a shared key authentication scheme, both STA and AP should have the correct shared secret key; this key is used to encrypt confidential information. The length of this key is 40-bits; this is a very short key length.

The main drawback of WEP is the use of this 40-bit key even though RC4 encryption algorithm can support up to 104 bit key but 40-bit key is the default key size shipped with WLAN products. Using key sizes higher then 40-bit is possible but it will cause problems when communicating with other devices because other devices might be using the default setting, which is 40-bits. WEP is still considered weak even if it uses 104-bit key for encryption, the key can be disclosed in less then 15 Minutes .

Another problem with WEP is the use of a short Initialization Vector (IV), typically 24-bit, not to mention that it is sent in the clear and it is being reused multiple numbers of times. The WEP encryption key, also called the RC4 key stream, is generated from the concatenation of the short shared secret 40-bits key and 24-bit IV. The 64-bit WEP encryption key stream and the 40-bit shared secret keys are the secret elements in the security system. Due to the short shared key length (40-bits), the frequent reuse of this key, short IV length, and again the frequent reuse of IV value, the generated WEP encryption key stream repeats it self after a period of time which means that the cipher text generated by The cipher text (C) is generated from a simple XOR operation between the WEP encryption key (K) and the plain text message (M) as illustrated in equation (1) and Figure 3. XORing the cipher text with the plain text message will result in the encryption key as illustrated equation (2). XORing two cipher text messages is equal to XORing two plain text messages as shown in equation (3). If one of the plain text messages is known, or at least parts of it, finding the WEP encryption key will becomes trivial [24]. Knowledge of plain text message and its corresponding cipher text message can be easily done by eavesdropping the initial challenge sent from the AP to the STA and the reply of that challenge. this key stream is easily breakable. Figure 3 shows the operation of WEP. WEP also provides simple integrity service (not shown in Figure 3), a checksum value is calculated for the message using a special Integrity Algorithm, and this checksum, also called Integrity Check Value ICV, is attached to the message. The receiver runs the same integrity algorithm on the message to output its own ICV then it compares it with the received ICV. The message is assured to be errorfree when both ICVs are identical.



The main problem here is that there is a direct relationship between WEP encryption keys and the IV used in a single session, so it is easy for an attacker who knows the WEP encryption key (using equations 1-3) to capture its corresponding IV. Because the length of the WEP encryption key and IVs are short, they are going to be repeated after a while. The attacker can build a database of IV's and their corresponding WEP keys. The attacker can monitor encrypted transmissions and captures IVs, lookup the corresponding WEP key and easily decrypts the transmission. This scheme is shown in Figure 4.



WEP also lacks key management solutions, there is no solid key distribution policy and a single key is reused frequently. This problem will not only make the AP vulnerable to attacks but it will make all other APs and STAs vulnerable as well. Even worse, key distribution is static by default which means all STAs have to have the key entered manually and when the key compromised, all STAs have to revoke it and use a new key. Generally, WEP lacks key management and distribution system. Reference [37] provides a possible solution to key distribution problem by distributing the keys by Dynamic Host Configuration Protocol (DHCP) server. DHCP server distributes WEP keys as part of DHCP frame options. WEP does not provide a defense mechanism against replay attacks. An attacker can record a WEP encrypted message and illegally use it later on in a multiple number of times to derive information about the encryption key or to access the WLAN as a legitimate user. It has been proved mathematically and practically that WEP is insecure at all and it is not recommended if high security is required. Nonetheless, WEP protected WLANs adds a hurdle against attackers and definitely such WLANs are better then non WEP-protected WLANs.

**Q5: Write short note on IEEE 802.11 standards.**

**Ans:-**

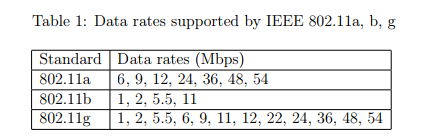
In 1997, IEEE approved 802.11, the first sanctioned WLAN standard. This first standard allowed three possible implementations for the physical layer: infrared (IR) pulse position modulation, or radio frequency (RF) signalling in the 2.4 GHz band using either Frequency Hopping Spread Spectrum (FHSS) or Direct Sequence Spread Spectrum (DSSS) . The IR method was never commercially implemented. The RF versions suffered from low transmission speeds.

IEEE established two networking groups (A and B) to explore alternate implementations of 802.11. A third group, working group G, was set up after these two.

Group A explored the 5 GHz band, using Orthogonal Frequency Division Multiplexing (OFDM) to achieve transmission rates in the range of 54 Mbps. The 802.11a standard was ratified in 1999. Due to slow availability of cheap 5 GHz components (required for keeping the cost of products low) and international regulations, the 802.11a WLAN standard did not reach the market before mid-2002.

Group B explored more sophisticated DSSS techniques in the original 2.4 GHz band. Their 802.11b WLAN standard, published in 1999, can deliver data rates up to 11 Mbps. Most WLAN systems in the market today follow the 802.11b WLAN standard.

Group G began by exploring a variety of methods to further improve throughput in the 2.4 GHz spectrum used by the 802.11b standard. In 2003, group G ratified the 802.11g standard adopting OFDM, the same signalling method used in the 802.11a WLAN standard. The 802.11g standard provides backward compatibility with the older 802.11b standard, which uses the same spectrum. Even though 802.11g operates in the same frequency band as 802.11b, it can achieve higher data rates because of its similarities to 802.11a. The maximum range of 802.11g devices is slightly greater than that of 802.11b devices, but the range in which a client can 5 Table 1: Data rates supported by IEEE 802.11a, b, g Standard Data rates (Mbps) 802.11a 6, 9, 12, 24, 36, 48, 54 802.11b 1, 2, 5.5, 11 802.11g 1, 2, 5.5, 6, 9, 11, 12, 22, 24, 36, 48, 54 achieve full data rate speed (54 Mbps) is much shorter than that of 802.11b. The MAC layers of 802.11a, b, and g protocols are identical. Each portion of the radio spectrum is called a channel. Most designers use one or more channels between 1 and 11 for deploying 802.11 WLANs. To overcome signal degradation, 802.11 WLANs can step down to a slower but more robust transmission rate when conditions are poor, then step back up again when conditions improve. Data rates supported by the 802.11 WLAN standard are shown in Table 1.

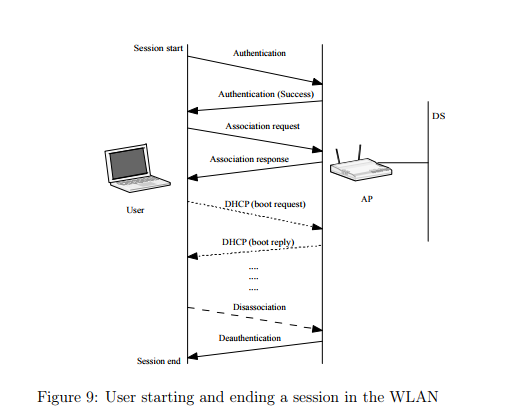


**Q6: Explain 802.11 MAC management functions. Explain in detail Power Management function with neat diagram.**

**Ans:-**

The following are the common management frame subtypes

* 1. Beacon: Beacon frames announce the existence of a network. They are transmitted at regular intervals to allow mobile stations to find and identify a network and possibly join it. In an infrastructure network, the AP is responsible for transmitting Beacon frames with information such as timestamp, SSID, and other parameters regarding the AP to stations that are within range.
  2. Authentication: Authentication frames are sent back and forth between the station requesting authentication and the station to which it is attempting to assert its authentic identity. With open system authentication, the station sends only one authentication frame, and the AP responds with an authentication frame as a response indicating acceptance or rejection.
  3. Deauthentication: This frame is an announcement stating that the receiver is no longer authenticated. It is a one-way communication from the authenticating station and must be accepted. It takes effect immediately.
  4. Association request: This frame carries information about the station (e.g., supported data rates) and the SSID of the network with which it wishes to associate. After receiving the association request, the AP considers associating with the station, and (if accepted) reserves memory space and establishes an association ID for the station. The sender must already be authenticated to obtain a successful association.
  5. Association response: An AP sends an association response frame containing an acceptance or rejection notice to the station requesting association. If the AP accepts the station, the frame includes information regarding the association, such as association ID and supported data rates. If the outcome of the association is positive, the station can utilise the AP to communicate with other stations on the network and systems on the DS.
  6. Reassociation request: If a station roams away from the currently associated AP and finds another AP having a stronger beacon signal, the station will send a reassociation frame to the new AP. The new AP then coordinates the forwarding of data frames that may still be in the buffer of the previous AP waiting for transmission to the station.
  7. Reassociation response: An AP sends a reassociation response frame containing an acceptance or rejection notice to the station requesting reassociation. Similar to the association process, the frame includes information regarding the association, such as association ID and supported data rates.
  8. Disassociation: A station sends a disassociation frame to another station if it wishes to terminate the association. For example, a station that is shutting down can “politely” send a disassociation frame to alert the AP that the station is powering off. The AP can then relinquish memory allocations and remove the radio station from the association table.



**Power management function**

Power Saving Wireless LANs are typically related to mobile applications. In this type of application, battery power is a scare resource. This is the reason why the 802.11 standard directly addresses the issue of Power Saving and defines an entire mechanism which enables stations to go into sleep mode for long periods of time without losing information. The main idea behind the Power Saving Mechanism is that the AP maintains a continually updated record of the stations currently working in Power Saving mode, and buffers the packets addressed to these stations until either the stations specifically request the packets by sending a polling request, or until they change their operation mode. As part of its Beacon Frames, The AP also periodically transmits information about which Power Saving Stations have frames buffered at the AP, so these stations wake up in order to receive the Beacon Frame. If there is an indication that there is a frame stored at the AP waiting for delivery, then the station stays awake and sends a Polling message to the AP to get these frames. Multicasts and Broadcasts are stored by the AP, and transmitted at a pre-known time (each DTIM), when all Power Saving stations who wish to receive this kind of frames are awake.

**Q7:Extra Questions:**

**Explain Physical layer of IEEE 802.11 WLAN**

Ans:-

## ****Physical layer functions****

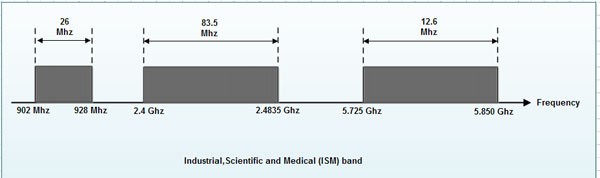
* 1. As we know that physical layer is responsible for converting data stream into signals, the bits of 802.11 networks can be converted to radio waves or infrared waves.
  2. These are six different specifications of IEEE 802.11. These implementations, except the first one, operate in *industrial, scientific*and *medical (ISM)*band. These three banks are unlicensed and their ranges are

1.902-928 MHz

2.2.400-4.835 GHz

3.5.725-5.850 GHz

c The different implementations of IEE802.11 are given below:-

[](http://ecomputernotes.com/images/ISM-Band.jpg)

## 1. IEEE 802.11 infrared

* 1. It uses diffused (not line of sight) infrared light in the range of 800 to 950 nm.
  2. It allows two different speeds: I Mbps and 2Mbps.
  3. For a I-Mbps data rate, 4 bits of data are encoded into 16 bit code. This 16 bit code contains fifteen as and a single 1.
  4. For a 2-Mbps data rate, a 2 bit code is encoded into 4 bit code. This 4 bit code contains three Os and a single 1.
  5. The modulation technique used is pulse position modulation (PPM) *i.e.*for converting digital signal to analog.

## 2. IEEE 802.11 FHSS

* 1. IEEE 802.11 uses Frequency Hoping Spread Spectrum (FHSS) method for signal generation.
  2. This method uses 2.4 GHz ISM band. This band is divided into 79 subbands of 1MHz with some guard bands.
  3. In this method, at one moment data is sent by using one carrier frequency and then by some other carrier frequency at next moment. After this, an idle time is there in communication. This cycle is repeated after regular intervals.
  4. A pseudo random number generator selects the hopping sequence.
  5. The allowed data rates are 1 or 2 Mbps.
  6. This method uses frequency shift keying (two level or four level) for modulation *i.e.*for converting digital signal to analogy.

## 3. IEEE 802.11 DSSS

* 1. This method uses Direct Sequence Spread Spectrum (DSSS) method for signal generation. Each bit is transmitted as 11 chips using a Barker sequence.
  2. DSSS uses the 2.4-GHz ISM band.
  3. It also allows the data rates of 1 or 2 Mbps.
  4. It uses phase shift keying (PSK) technique at 1 M baud for converting digital signal to analog signal.

## ****4. IEEE 802.11a OFDM****

* 1. This method uses Orthogonal Frequency Division Multiplexing (OFDM) for signal generation.
  2. This method is capable of delivering data upto 18 or 54 Mbps.
  3. In OFDM all the subbands are used by one source at a given time.
  4. It uses 5 GHz ISM band.
  5. This band is divided into 52 subbands, with 48 subbands for data and 4 subbands for control [information](http://ecomputernotes.com/fundamental/information-technology/what-do-you-mean-by-data-and-information).
  6. If phase shift keying (PSK) is used for modulation then data rate is 18 Mbps. If quadrature amplitude modulation (QAM) is used, the data rate can be 54 Mbps.

## ****5. IEEE 802.11b HR-OSSS****

* 1. It uses High Rate Direct Sequence Spread Spectrum method for signal generation.
  2. HR-DSSS is similar to DSSS except for encoding method.
  3. Here, 4 or 8 bits are encoded into a special symbol called complementary code key (CCK).
  4. It uses 2.4 GHz ISM band.
  5. It supports four data rates: 1,2,5.5 and 11 Mbps.
  6. 1 Mbps and 2 Mbps data rates uses phase shift modulation.
  7. The 5.5. Mbps version uses BPSK and transmits at 1.375 Mbaud/s with 4-bit CCK encoding.
  8. The 11 Mbps version uses QPSK and transmits at 1.375 Mbps with 8-bit CCK encoding.

## ****6. IEEE 802.11g OFDM****

* 1. It uses OFDM modulation technique.
  2. It uses 2.4 GHz ISM band.
  3. It supports the data rates of 22 or 54 Mbps.
  4. It is backward compatible with 802.11 b.

**5: Wireless Personal Area Network**

**Q1: Explain in detail LRWPAN.**

**Ans:-**

The IEEE 802.15.4 has been designed to be useful in a wide variety of applications. These include automotive sensing, such as tire pressure monitoring; precision agriculture, such as the sensing of soil moisture. The largest application opportunities are in home automation and networking including heating, air conditioning; the control of objects such as curtains, windows; health monitoring, including diagnostics; and toys and games.

1. **IEEE 802.15 LR-WPAN Device Architecture**

i. The device comprises a physical layer (PHY), which contains the RF transceiver along with its low-level control mechanism.

ii. A MAC sublayer provides access to the physical channel for all types of transfer.

iii. The upper layers consist of a network layer, which provides network configuration, manipulation, and message routing.

iv. The application layer provides the intended function of a device.

v. An IEEE 802.2 logical link control (LLC) can access the MAC through the service specific convergence sublayer (SSCS).

**2. Physical Layer**

i. The PHY provides two services: the PHY data service and PHY management service interfacing to the physical layer management entity (PLME).

ii. The PHY data service enables the transmission and reception of PHY protocol data units (PPDUs) across the physical radio channel.

iii. The PHY management services are activation and deactivation of the radio transceiver, energy detection (ED), link quality indication (LQI), channel selection, clear channel assessment (CCA).

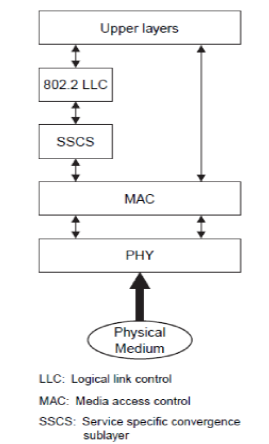
iv. There are three frequency bands: 2.4GHz global, 915MHz America and 868MHz Europe. There is a single channel between 868 and 868.6 MHz, 10 channels between 902 and 928 MHz, and 16 channels between 2.4 and 2.4835 GHz.

v. The data rate is 250 kbps at 2.4 GHz, 40 kbps at 915 MHz, and 20 kbps at 868 MHz Receiver sensitivities are -85 dBm for 2.4 GHz and -92 dBm for 868/915 MHz.

vi. The range of 10-20 meters is covered.

vii. To maintain a common simple interface with MAC, both PHY data service and management service share a single packet structure.

viii. A typical packet size for home applications is of the order of 30-60 bytes. More demanding applications such as interactive games require larger size packets. (127 bytes maximum)



**Fig8. IEEE 802.15 LR-WPAN Device Architecture**

ix. The maximum packet durations are 4.25 ms for the 2.4 GHz band, 26.6 ms for the 915 MHz band, and 53.2 ms for the 868 MHz band.

x. The standard provides two options based on the frequency band. Both are based on direct sequence spread spectrum (DSSS).

xi. The 868/915 MHz PHY uses a simple DSSS approach in which each transmitted bit is represented by a 15-chip maximum length sequence with BPSK modulation.

xii. The 2.4 GHz PHY uses a 16-ary quasi-orthogonal modulation technique based on DSSS methods with OQPSK modulation.

**3. Data link Layer**

i. The data link layer is divided into two sublayers, the MAC and LLC sublayers.

ii. The logical link control is standardized in IEEE 802.2 and is common among all IEEE 802 standards.

iii. The MAC provides services to an IEEE 802.2 type logical link control through the service-specific convergence sublayer (SCCS), or a proprietary LLC can access the MAC services directly without going through the SCCS.

iv. The SCCS ensures compatibility between different LLC sublayers and allows the MAC to be accessed through a single set of access points.

v. The features of the MAC are association and disassociation, acknowledged frame delivery, channel access mechanism, frame validation, guaranteed time slot management, and beacon management.

vi. The MAC provides two services to higher layers that can be accessed through two service access points (SAPs). The MAC data service is accessed through the MAC common part sublayer (MCPS-SAP), and the MAC management services are accessed through the MAC layer management entity (MLME-SAP). These two services provide an interface between the SCCS or another LLC and the physical layer.

vii. An important function of the MAC is to confirm successful reception of a received frame. Successful reception and validation of a data or MAC command frame is confirmed with an acknowledgment.

viii. Three levels of security are provided: no security of any type; access control lists (non-cryptographic security); and symmetric key security, using AES-128.

**4. Network Layer**

i. The network layer of Zigbee (IEEE 802.15.4) is responsible for topology construction and maintenance as well as naming and binding services, which include the tasks of addressing, routing, and security.

ii. IEEE 802.15.4 supports multiple network topologies, including star, peer-to-peer, and cluster tree. The topology is an application design choice.

**Q2: Explain in detail Bluetooth Architecture. Or Protocol Architecture**

**Ans:-**

**1. Transport protocol group:** .

The protocols in this group are designed to

1. Allow devices to locate and connect
2. Carry audio and data traffic where audio traffic has higher priority.
3. Support synchronous and asynchronous transmission for telephony grade voice communication
4. Manage physical and logical links between devices so that layers above and applications can pass data through connections.
5. The following protocols are in this group:

i. Logical link control and adaptation protocol layer (L2CAP)

1. All data traffic is routed through this layer.
2. This layer shields higher layers from details of lower layers.
3. It segments larger packets from higher layers into smaller packets that can be easily handled by lower layers.
4. It facilitates maintenance of desired grade of service in two peer devices.

ii. Link manager layer (LML)

1. It negotiates properties of Bluetooth air interface between communicating devices.
2. These properties may be bandwidth allocation, support services of particular type, etc.
3. This layer also supervises devices pairing.
4. Device pairing generates and stores authentication key specific to a device
5. It is also responsible for power control and may request adjustments in power levels.

iii. Baseband and radio layers

1. The baseband layer is responsible for searching other devices, assigning master and slave roles.
2. This layer also controls Bluetooth unit’s synchronization and transmission frequency hopping sequence. It manages link between devices and determines packet types supported for synchronous and asynchronous traffic.

iv. Host Controller Interface (HCI)

1. The HCI allows higher layers of stack, including applications, to access the baseband, link manager, etc., through a single standard interface.
2. It serves the purpose of interoperability between host devices and Bluetooth modules.
3. HCI commands, module may enter certain modes of operation. Higher layers are informed about certain events through HCI.

**2. Middleware protocol group**

1. The protocols in this group are needed for existing applications to operate over Bluetooth links.
2. These protocols may be third party protocols (Industry standard) or developed by ‘simple interest group (SIG)’ specifically for Bluetooth.
3. Some of the protocols in this group:

i. RFCOMM layer

1. It provides a virtual serial port for applications needed for scenarios like dial-up networking, etc.
2. This eliminates the use of cables.

ii. Service Discovery protocol layer (SDP)

1. The SDP is a standard method for Bluetooth devices to discover and learn about the services offered by other device once a connection is established with it.

iii. Infrared data association(IrDA) interoperability protocols

1. The SIG has adopted some IrDA protocols to ensure interoperability between applications to exchange a wide variety of data.

iv. Object exchange protocol (OBEX)

1. It is developed by IrDA to exchange objects simple and spontaneous manner.
2. It uses client-server model.
3. It is independent of transport mechanism and transport ‘Application programming Interface (API)’, provided it realizes a reliable transport base.
4. It defines a folder-listing object, which is used to browse contents of folders on a remote device.

v. Networking layers

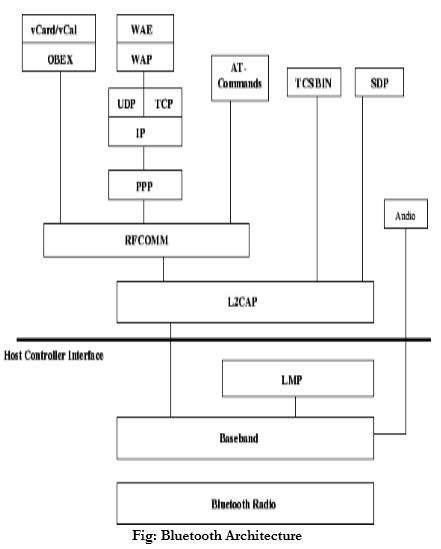
1. Bluetooth wireless technology uses peer-to-peer network topology.
2. Dial-up networking uses AT commands.
3. In most cases, network accessed is IP network with use of standard protocols like TCP, UDP, HTTP
4. A device can connect to IP network using network access point. The internet PPP is used to connect to access point.

vi. Telephone control specifications layer (TCS) and audio

1. This layer is designed to set up voice calls. It supports functions like call control and group management.
2. TCS can also be used to set up data calls.
3. TCS protocols are compatible with ITU Specifications.
4. Bluetooth audio communication takes place at rate of 64Kbps using one of two encoding schemes: 8-bit logarithmic PCM or continuous variable slope delta modulation.

**3. Application group**

1. This group consists of actual applications that make use of Bluetooth links and refers to software that exists above protocol stack.
2. The Bluetooth-SIG does not define any application protocols nor does it specify any API. Bluetooth profiles are developed to establish a base point for use of a protocol stack to accomplish a given usage case.



**Q3: Explain Bluetooth security aspects.**

Ans:-

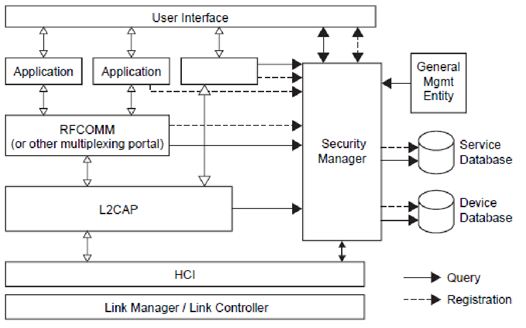
**1. Bluetooth security features**

Bluetooth security supports authentication and encryption. Authentication verifies who is at the other end of the link. Encryption ensures confidentiality of data. Even if a third party hacks the data, it is in encrypted form and not in original form.

i. Pairing: When two devices communicate for the first time, there is a pairing procedure. In this procedure, a secret key is generated. This key is shared by both the devices. It is stored in each device. When the devices want to communicate in future, there is no pairing procedure.

ii. Security modes of a device: There are three security modes to a device.

1. Non-secure: A device will not initiate any security procedure.
2. Service level enforced security: A device does not initiate security procedures before channel establishment at the L2CAP level.
3. Link level enforced security: A device initiates security procedures before link set up at LMP is completed.



**Fig2. Bluetooth Security Architecture**

**2. Bluetooth security levels**

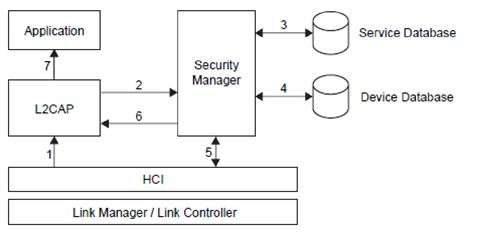
There are 2 kinds of security levels:

**Authentication and Authorization**

i. **Types of services:** Different services have different service requirements. Some services require authentication and authorization. Some services require only authentication and not authorization. Some services don’t require both authentication and authorization.

ii. **Authentication:** Authentication is performed after determining the type of service. It cannot be performed when ACL link is established. It is performed only when connection request to service is submitted. It can be performed in both directions: client authenticates server and vice versa.

iii. **Authentication procedure:** - Connection request to L2CAP is sent - L2CAP requests access from security manager - Security manager enquires the service database - Security manager enquires the device database - If necessary, security manager enforces the authentication and encryption procedure. - The security manager grants access and L2CAP continues to set up the connection.



**Fig3. Authentication Procedures**

**iv. Authorization:**

Some services require manual authorization of the device after authentication only then, these services can be accessed. This leads to the concept of trust. There are two kinds of device trust levels:

1. Trusted device: It has fixed relationship (paired) and unrestricted access to all services.
2. Untrusted device: This device has been previously authenticated, a link key is stored, but the device is not marked as trusted in device database.
3. An unknown device is also an untrusted device. No security information is available for this device.

**Q4:Write short note on Wireless Sensor Network**

Ans:-

**1. Replacement of Wired sensor networks**

i. Wired sensor networks include gauges measuring temperature, fluid levels, humidity, and other attributes on pipelines, pumps, generators, and manufacturing lines.

ii. Many of these run as separately wired networks, sometimes linked to a computer but often to a control panel that flashes lights or sounds an alarm when a temperature rises too high or a machine vibrates too much.

iii. Also wired in are actuators, which let the control panel slow down a pump or start a fan in response to the sensor data.

iv. With advances in silicon radio chips, cleverly designed routing algorithms and network software; wireless sensor networks are in use.

v. Wireless sensor networks eliminate wires and their installation and maintenance costs.

vi. Wireless sensor networks can use several different wireless technologies, including IEEE 802.11 WLANs, Bluetooth, and radio frequency identification (RFID).

vii. However, most of the applications use low-power radios having a range of about 30 to 200 feet and data rates of up to around 300 kbps.

**2. Sensor nodes**

i. A wireless sensor network contains a large number of tiny sensor nodesthat are densely deployed either inside the phenomenon to be sensed or very close to it.

ii. Sensor nodes consist of sensing, data processing, and communicating components.

iii. The position of sensor nodes need not be engineered or predetermined.

iv. This allows random deployment in inaccessible terrain or disaster relief operations.

v. Thus the sensor network protocols and algorithms must possess self-organizing capabilities.

vi. Another unique feature of sensor networks is the cooperative effort of sensor nodes. Sensor nodes are fitted with an inboard processor. Instead of sending the raw data to the nodes responsible for the fusion, they use their processing abilities to locally carry out simple computations and transmit only required and partially processed data.

**3. Wireless ad-hoc network**

i. Wireless sensor network applications require wireless ad hoc networking techniques.

ii. However, there are many differences between wireless sensor network and wireless ad hoc networks.

iii. The number of sensor nodes in a wireless sensor network can be several orders of magnitude higher than the nodes in a wireless ad hoc network.

iv. In a wireless sensor network, sensor nodes are densely deployed.

v. Sensor nodes are prone to failure.

vi. The topology of a wireless sensor network changes very frequently.

vii. Sensor nodes mainly use broadcast communication paradigms whereas most traditional ad hoc networks are based on point-to-point communications.

viii. Sensor nodes are limited in power, computational capabilities, and memory.

ix. Sensor nodes may not have global identification because of the large amount of overhead and large number of sensors.

x. Another factor that distinguishes wireless sensor networks from traditional mobile ad hoc networks (MANETs) is that the end goal is the detection/estimation of some event(s) of interest, and not just communication.

xi. To improve detection performance, it is often quite useful to fuse data from multiple sensors. Data fusion requires the transmission of data and control messages. This need may impose constraints on network architecture.

xii. The large number of sensing nodes may congest the network with information. To solve this problem, some sensors, such as cluster heads, can aggregate the data, perform some computation (e.g., average, summation, highest value, etc.), and then broadcast the summarized new information.

**4. Low power consumption**

i. Since large numbers of sensor nodes are densely deployed, neighbour nodes may be very close to each other. Hence, multihop communication in wireless sensor networks is expected to consume less power than traditional single hop communication.

ii. Furthermore, the transmission power level can be kept low, which is highly desirable in covert operations. Multihop communication can effectively overcome some of the signal propagation effects experienced in long-distance wireless communication.

iii. One of the most important constraints on sensor nodes is the low power consumption requirement.

iv. Sensor nodes carry limited, generally irreplaceable power sources.

v. Therefore, while traditional networks aim to achieve high quality of service (QoS) provisions, wireless sensor network protocols must focus primarily on power conservation.

vi. They must have built-in trade-off mechanisms that give the end-user the option of prolonging network lifetime at the cost of lower throughput or higher transmission delay.

**6: Wireless Metropolitan Area Network**

**Q1: Write short note on WiMAX or**

**Explain WiMax system and compare the different 802.16 standards.**

Ans:-

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

**Q2: Give in detail comparison between WiMAX and LTE/3GPP.**

Ans:-

|  |
| --- |
|  |
|  |

**7: Security in Wireless Network**

**Q1: Explain possible attacks on Wireless LAN and explain WEP in detail.**

**Or**

**Explain WEP protocol in detail.**

**Or**

**Explain the wired Equivalent Privacy Protocol. Also explain WEP security based on the access control list with neat diagram.**

**Ans:-** **Wireless attacks are of two sub categories:**

**1] Passive:-eavesdropping or snooping on transmission.**

**2] Active:- Altering data or creating fraudulent streams.**

**List of attacks:-**

**1. Interruption of service**

**2. Modification**

**3. Fabrication**

**4. Interception**

**5. Jamming**

**6. Client-to-client attacks.**

**7. Attacks against encryption**

**8. Misconfiguration**

**9. Brute force attack against passwords of access points.**

**10. Insertion attacks.**

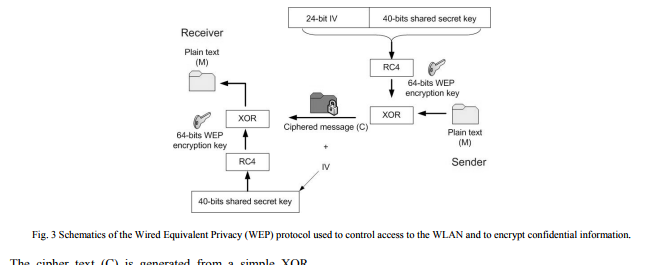
**(\*Explain in one sentence above all attackes)**

**WEP:-**

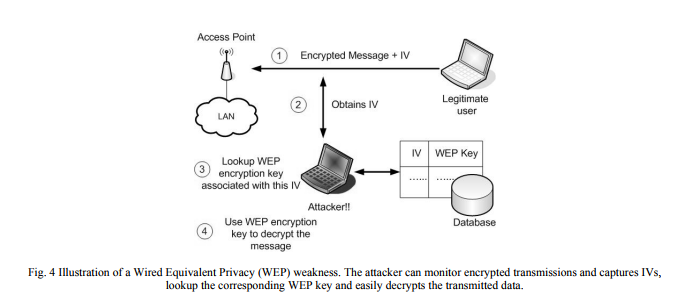
Wired Equivalent Privacy (WEP): WEP is the security protocol in use since the early IEEE802.11 standard . It is used to secure communications between APs and STAs and to provide secured authentication schemes; the aim was to provide security to the WLAN similar to the security provided in the wired LAN. It is based on a stream cipher encryption algorithm called "RC4". WEP is used to control access to the WLAN and to encrypt confidential information. It was proved theoretically and practically that WEP failed as a security protocol because of many problems. To access a WLAN in a shared key authentication scheme, both STA and AP should have the correct shared secret key; this key is used to encrypt confidential information. The length of this key is 40-bits; this is a very short key length.

The main drawback of WEP is the use of this 40-bit key even though RC4 encryption algorithm can support up to 104 bit key but 40-bit key is the default key size shipped with WLAN products. Using key sizes higher then 40-bit is possible but it will cause problems when communicating with other devices because other devices might be using the default setting, which is 40-bits. WEP is still considered weak even if it uses 104-bit key for encryption, the key can be disclosed in less then 15 Minutes .

Another problem with WEP is the use of a short Initialization Vector (IV), typically 24-bit, not to mention that it is sent in the clear and it is being reused multiple numbers of times. The WEP encryption key, also called the RC4 key stream, is generated from the concatenation of the short shared secret 40-bits key and 24-bit IV. The 64-bit WEP encryption key stream and the 40-bit shared secret keys are the secret elements in the security system. Due to the short shared key length (40-bits), the frequent reuse of this key, short IV length, and again the frequent reuse of IV value, the generated WEP encryption key stream repeats it self after a period of time which means that the cipher text generated by The cipher text (C) is generated from a simple XOR operation between the WEP encryption key (K) and the plain text message (M) as illustrated in equation (1) and Figure 3. XORing the cipher text with the plain text message will result in the encryption key as illustrated equation (2). XORing two cipher text messages is equal to XORing two plain text messages as shown in equation (3). If one of the plain text messages is known, or at least parts of it, finding the WEP encryption key will becomes trivial [24]. Knowledge of plain text message and its corresponding cipher text message can be easily done by eavesdropping the initial challenge sent from the AP to the STA and the reply of that challenge. this key stream is easily breakable. Figure 3 shows the operation of WEP. WEP also provides simple integrity service (not shown in Figure 3), a checksum value is calculated for the message using a special Integrity Algorithm, and this checksum, also called Integrity Check Value ICV, is attached to the message. The receiver runs the same integrity algorithm on the message to output its own ICV then it compares it with the received ICV. The message is assured to be errorfree when both ICVs are identical.



The main problem here is that there is a direct relationship between WEP encryption keys and the IV used in a single session, so it is easy for an attacker who knows the WEP encryption key (using equations 1-3) to capture its corresponding IV. Because the length of the WEP encryption key and IVs are short, they are going to be repeated after a while. The attacker can build a database of IV's and their corresponding WEP keys. The attacker can monitor encrypted transmissions and captures IVs, lookup the corresponding WEP key and easily decrypts the transmission. This scheme is shown in Figure 4.



WEP also lacks key management solutions, there is no solid key distribution policy and a single key is reused frequently. This problem will not only make the AP vulnerable to attacks but it will make all other APs and STAs vulnerable as well. Even worse, key distribution is static by default which means all STAs have to have the key entered manually and when the key compromised, all STAs have to revoke it and use a new key. Generally, WEP lacks key management and distribution system. Reference [37] provides a possible solution to key distribution problem by distributing the keys by Dynamic Host Configuration Protocol (DHCP) server. DHCP server distributes WEP keys as part of DHCP frame options. WEP does not provide a defense mechanism against replay attacks. An attacker can record a WEP encrypted message and illegally use it later on in a multiple number of times to derive information about the encryption key or to access the WLAN as a legitimate user. It has been proved mathematically and practically that WEP is insecure at all and it is not recommended if high security is required. Nonetheless, WEP protected WLANs adds a hurdle against attackers and definitely such WLANs are better then non WEP-protected WLANs.

**Q2: Write short note on VPN.**

**Ans:-**

**VPN** is a private connection between two machines or networks over a shared or public network. VPN technology lets an organization securely extend its network services over the Internet to remote users, branch offices, and partner companies. VPN turn the Internet into a simulated private WAN.

VPN allows users working at home or office to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public inter-network (such as the Internet). From the user's perspective, the VPN is a point-to-point connection between the user's [computer](http://ecomputernotes.com/fundamental/introduction-to-computer/what-is-computer) and a corporate server. The nature of the intermediate inter-network is irrelevant to the user because it appears as if the data is being sent over a dedicated private link.

Data sent across the public Internet is generally not protected from curious eyes, but you can make your Internet communications secure and extend your private network with a virtual private network (VPN) connection. VPN uses a technique known as tunneling to transfer data securely on the Internet to a remote access.

The Internet connection over the VPN is encrypted and secure. New authentication and encryption protocols are enforced by the remote access server. Sensitive data is hidden from the public, but it is securely accessible to appropriate users through a VPN.

There are following two ways to create a VPN connection:

1. By dialing an Internet service provider (ISP)

If you dial-in to an ISP, your ISP then makes another call to the private network's remote access server to establish the PPTP or L2TP tunnel after authentication, you can access the private network.

1. By connecting directly to the Internet

If you are already connected to an Internet, on a local area network, a cable modem, or a digital subscriber line (DSL), you can make a tunnel through the Internet and connects directly to the remote access server. After authentication, you can access the corporate network.

## ****Features of a Typical VPN solution****

When the remote offices connect each other to share vital resources and secret information, the VPN solution must ensure the privacy and integrity of the data as it traverses the Internet.

**Therefore, a VPN solution must provide at least all of the following:**

1. **Keep data confidential** (encryption)
2. Data carried on the public network must be rendered unreadable to unauthorized clients on the network.
3. **Ensure the identities of two parties communicating**(authentication)
4. The solution must verify the user's identity and restrict VPN access to authorized users only. It must also provide audit and accounting records to show who accessed what information and when.
5. **Safeguard the identities of communicating parties** (tunneling)
6. **Guard against packets being sent over and over** (replay prevention)
7. **Ensure data is accurate and in its original form** (non-repudiation)

**Address Management.** The solution must assign a client's address on the private net and ensure that private addresses are kept private.

**Key Management.** The solution must generate and refresh encryption keys for the client and the server.

**Multiprotocol Support.**The solution must handle common protocols used in the public network. These include IP, Internet Packet Exchange (IPX), and so on.

An Internet VPN solution based on the Point-to-Point Tunneling Protocol (PPTP) or Layer 2 Tunneling Protocol (L2TP) meets all of these basic requirements and takes advantage of the broad availability of the Internet. Other solutions, including the new IP Security Protocol (IPsec), meet only some of these requirements, but remain useful for specific situations.

## ****Benefits of VPN****

The main benefit of a VPN is the potential for significant cost savings compared to traditional leased lines or dial up networking. These savings come with a certain (in amount of risk, however, particularly when using the public Internet as the delivery mechanism for VPN data.

The performance of a VPN will be more unpredictable and generally slower than dedicated lines due to public Net traffic. Likewise, many more points of failure can affect a Net-based VPN than in a closed private system. Utilizing any public network for communications naturally raises new security concerns not present when using more controlled environments like point-to-point leased lines.

**Q3: Write short note on Mobile IP.**

**Ans:-**

**Introduction**

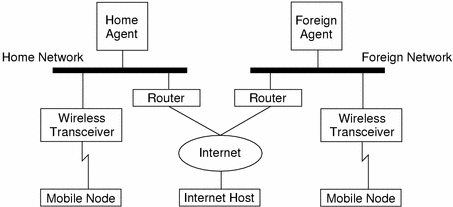
Current versions of the Internet Protocol (IP) assume that the point at which a computer attaches to the Internet or a network is fixed and its IP address identifies the network to which it is attached. Datagrams are sent to a computer based on the location information contained in the IP address.

If a mobile computer, or **mobile node**, moves to a new network while keeping its IP address unchanged, its address does not reflect the new point of attachment. Consequently, existing routing protocols cannot route datagrams to the mobile node correctly. In this situation, you must reconfigure the mobile node with a different IP address representative of its new location, which is a cumbersome process. Thus, under the current Internet Protocol, if the mobile node moves without changing its address, it loses routing; but if it does change its address, it loses connections.

Mobile IP solves this problem by allowing the mobile node to use two IP addresses: a fixed **home address** and a **care-of address** that changes at each new point of attachment. Mobile IP enables a computer to roam freely on the Internet or an organization's network while still maintaining the same home address. Consequently, computing activities are not disrupted when the user changes the computer's point of attachment to the Internet or an organization's network. Instead, the network is updated with the new location of the mobile node. See [Glossary](https://docs.oracle.com/cd/E19455-01/806-7600/6jgfbep2o/index.html) for definitions of terms associated with Mobile IP.

The following figure illustrates the general Mobile IP topology.

**Figure 1–1 Mobile IP Topology**



Using the previous illustration's Mobile IP topology, the following scenario shows how a datagram moves from one point to another within the Mobile IP framework.

1. The Internet host sends a datagram to the mobile node using the mobile node's home address (normal IP routing process).
2. If the mobile node is on its home network, the datagram is delivered through the normal IP process to the mobile node. Otherwise, the home agent picks up the datagram.
3. If the mobile node is on a foreign network, the home agent forwards the datagram to the foreign agent.
4. The foreign agent delivers the datagram to the mobile node.
5. Datagrams from the mobile node to the Internet host are sent using normal IP routing procedures. If the mobile node is on a foreign network, the packets are delivered to the foreign agent. The foreign agent forwards the datagram to the Internet host.

In the case of wireless communications, the illustrations depict the use of wireless transceivers to transmit the datagrams to the mobile node. Also, all datagrams between the Internet host and the mobile node use the mobile node's home address regardless of whether the mobile node is on a home or foreign network. The care-of address is used only for communication with mobility agents and is never seen by the Internet host.

**Mobile IP Functional Entities**

Mobile IP introduces the following new functional entities:

**1. Mobile Node (MN)**–Host or router that changes its point of attachment from one network to another.

**2. Home Agent (HA)**–Router on a mobile node's home network that intercepts datagrams destined for the mobile node, and delivers them through the care-of address. The home agent also maintains current location information for the mobile node.

**3. Foreign Agent (FA)**–Router on a mobile node's visited network that provides routing services to the mobile node while the mobile node is registered.

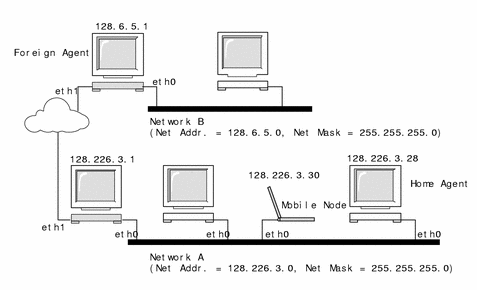
**How Mobile IP Works**

Mobile IP enables routing of IP datagrams to mobile nodes. The mobile node's home address always identifies the mobile node, regardless of its current point of attachment to the Internet or an organization's network. When away from home, a care-of address associates the mobile node with its home address by providing information about the mobile node's current point of attachment to the Internet or an organization's network. Mobile IP uses a registration mechanism to register the care-of address with a home agent.

The home agent redirects datagrams from the home network to the care-of address by constructing a new IP header that contains the mobile node's care-of address as the destination IP address. This new header then encapsulates the original IP datagram, causing the mobile node's home address to have no effect on the encapsulated datagram's routing until it arrives at the care-of address. This type of encapsulation is also called **tunneling**. After arriving at the care-of address, each datagram is de-encapsulated and then delivered to the mobile node.

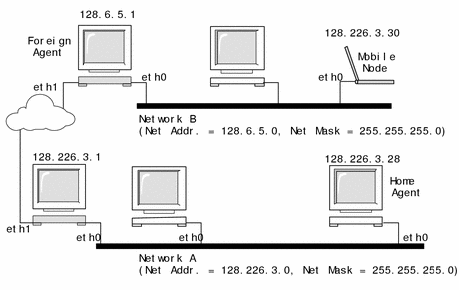
The following illustration shows a mobile node residing on its home network, Network A, before the mobile node moves to a foreign network,Network B. Both networks support Mobile IP. The mobile node is always associated with its home network by its permanent IP address, 128.226.3.30. Though Network A has a home agent, datagrams destined for the mobile node are delivered through the normal IP process.

**Figure 1–2 Mobile Node Residing on Home Network**



The following illustration shows the mobile node moving to a foreign network, Network B. Datagrams destined for the mobile node are intercepted by the home agent on the home network, Network A, encapsulated, and sent to the foreign agent on Network B. Upon receiving the encapsulated datagram, the foreign agent strips off the outer header and delivers the datagram to the mobile node visiting Network B.

**Figure 1–3 Mobile Node Moving to a Foreign Network**



The care-of address might belong to a foreign agent, or might be acquired by the mobile node through Dynamic Host Configuration Protocol (DHCP) or Point-to-Point Protocol (PPP). In the latter case, a mobile node is said to have a co-located care-of address.

The mobile node uses a special **registration** process to keep its home agent informed about its current location. Whenever a mobile node moves from its home network to a foreign network, or from one foreign network to another, it chooses a foreign agent on the new network and uses it to forward a registration message to its home agent.

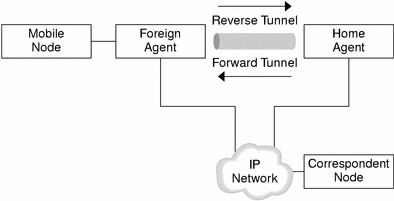
Mobility agents (home agents and foreign agents) advertise their presence using **agent advertisement** messages. A mobile node can optionally solicit an agent advertisement message from any locally attached mobility agents through an **agent solicitation** message. A mobile node receives these agent advertisements and determines whether they are on its home network or a foreign network.

When the mobile node detects that it is located on its home network, it operates without mobility services. If returning to its home network from being registered elsewhere, the mobile node **deregisters** with its home agent.

**Mobile IP with Reverse Tunneling**

The previous description of Mobile IP assumes that the routing within the Internet is independent of the data packet's source address. However, intermediate routers might check for a topologically correct source address. If an intermediate router does check, you should set up a reverse tunnel. By setting up a reverse tunnel from the mobile node's care-of address to the home agent, you ensure a topologically correct source address for the IP data packet. A mobile node can request a **reverse tunnel** between its foreign agent and its home agent when the mobile node registers. A reverse tunnel is a tunnel that starts at the mobile node's care-of address and terminates at the home agent. The following illustration shows the Mobile IP topology that uses a reverse tunnel.

**Figure 1–4 Mobile IP With a Reverse Tunnel**

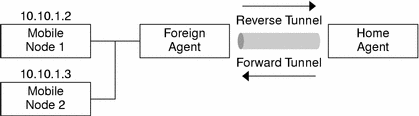


**Limited Private Addresses Support**

Mobile nodes that have private addresses which are not globally routable through the Internet require reverse tunnels. Solaris Mobile IP supports only privately addressed mobile nodes.

Enterprises employ private addresses when external connectivity is not required. Private addresses are not routable through the Internet. When a mobile node has a private address, the mobile node can only communicate with a correspondent node through a reverse tunnel. The privately addressed correspondent node must belong to the same home agent's administrative domain. The following illustration shows a network topology with two privately addressed mobile nodes that use the same care-of address when registered to the same foreign agent.

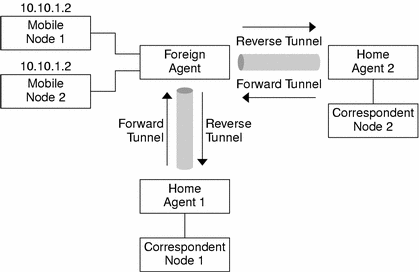
**Figure 1–5 Privately Addressed Mobile Nodes Residing on the Same Foreign Network**



Because both privately addressed mobile nodes belong to the same administrative domain, the home agent knows how to route data packets between the two mobile nodes. Also, the foreign agent's care-of address and the home agent's IP address must be globally routable addresses.

It is possible to have two privately addressed mobile nodes with the same IP address residing on the same foreign network. This situation is only possible when each mobile node has a different home agent. Also, this situation is only possible when each mobile node is on different advertising subnets of a single foreign agent. The following illustration shows a network topology that depicts this case.

**Figure 1–6 Privately Addressed Mobile Nodes Residing on Different Foreign Networks**



Because both privately addressed mobile nodes have the same IP address and because these mobile nodes belong to different home agent domains, the two nodes cannot communicate with each other. However, each node can communicate with nodes in its corresponding home agent's administrative domain through the reverse tunnel. For example, Mobile Node 2 can communicate with Correspondent Node 2 in the previous illustration.

**Care-of Addresses**

Mobile IP provides the following alternative modes for the acquisition of a care-of address:

1. A foreign agent provides a **foreign agent care-of address** through its agent advertisement messages. In this case, the care-of address is an IP address of the foreign agent. The foreign agent is the endpoint of the tunnel and, on receiving tunneled datagrams, de-encapsulates them and delivers the inner datagram to the mobile node. In this mode, many mobile nodes can share the same care-of address. This sharing reduces demands on the IPv4 address space and can also save bandwidth, because the forwarded packets, from the foreign agent to the mobile node, are not encapsulated. Saving bandwidth is important on wireless links.

2. A mobile node acquires a **co-located care-of address** as a local IP address through some external means, which the mobile node then associates with one of its own network interfaces. The address might be dynamically acquired as a temporary address by the mobile node, such as through DHCP. The address might also be owned by the mobile node as a long-term address for its use only while visiting some foreign network. When using a co-located care-of address, the mobile node serves as the endpoint of the tunnel and performs de-encapsulation of the datagrams tunneled to it.

Co-located care-of address enables a mobile node to function without a foreign agent, for example, in networks that have not yet deployed a foreign agent.

If a mobile node is using a co-located care-of address, the mobile node must be located on the link identified by the network prefix of this care-of address. Otherwise, datagrams destined to the care-of address are undeliverable.

**Agent Discovery**

A mobile node uses a method known as agent discovery to determine the following information:

1. When the node has moved from one network to another

2. Whether the network is the node's home or a foreign network

3. What is the foreign agent care-of address offered by each foreign agent on that network

Mobility agents transmit **agent advertisements** to advertise their services on a network. In the absence of agent advertisements, a mobile node can solicit advertisements. This is known as **agent solicitation**.

**Agent Advertisement**

Mobile nodes use agent advertisements to determine their current point of attachment to the Internet or to an organization's network. An agent advertisement is an Internet Control Message Protocol (ICMP) router advertisement that has been extended to also carry a mobility agent advertisement extension.

A foreign agent can be too busy to serve additional mobile nodes. However, a foreign agent must continue to send agent advertisements. This way, mobile nodes that are already registered with it will know that they have not moved out of range of the foreign agent and that the foreign agent has not failed.

Also, a foreign agent that supports reverse tunnels must send it's advertisements with the reverse tunnel flag set on.

**Agent Solicitation**

Every mobile node should implement agent solicitation. The mobile node uses the same procedures, defaults, and constants for agent solicitation, as specified for ICMP router solicitation messages.

The rate at which a mobile node sends solicitations is limited by the mobile node. The mobile node can send three initial solicitations at a maximum rate of one per second while searching for an agent. After registering with an agent, the rate at which solicitations are sent is reduced, to limit the overhead on the local network.

**Mobile IP Registration**

When the mobile node receives an agent advertisement, the mobile node registers through the foreign agent, even when the mobile node might be able to acquire its own co-located care-of address. This feature enables sites to restrict access to mobility services. Through agent advertisements, mobile nodes detect when they have moved from one subnet to another.

Mobile IP registration provides a flexible mechanism for mobile nodes to communicate their current reachability information to their home agent. The registration process enables mobile nodes to perform the following tasks:

1. Request forwarding services when visiting a foreign network
2. Inform their home agent of their current care-of address
3. Renew a registration that is due to expire
4. Deregister when they return home
5. Request a reverse tunnel

Registration messages exchange information between a mobile node, a foreign agent, and the home agent. Registration creates or modifies a mobility binding at the home agent, associating the mobile node's home address with its care-of address for the specified lifetime.

The registration process also enables mobile nodes to:

1. Register with multiple foreign agents
2. Deregister specific care-of addresses while retaining other mobility bindings
3. Discover the address of a home agent if the mobile node is not configured with this information

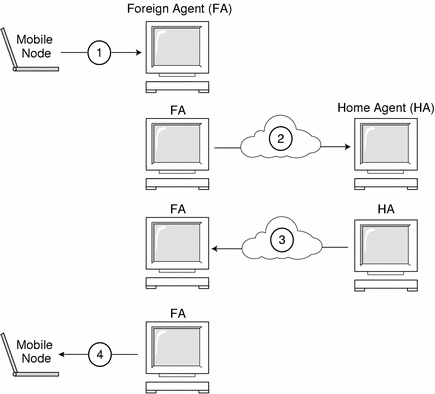
Mobile IP defines the following registration processes for a mobile node:

1. If a mobile node is registering a foreign agent care-of address, the mobile node registers using that foreign agent.
2. If a mobile node is using a co-located care-of address, and receives an agent advertisement from a foreign agent on the link on which it is using this care-of address, the mobile node registers using that foreign agent (or another foreign agent on this link).
3. If a mobile node uses a co-located care-of address, the mobile node registers directly with its home agent.
4. If a mobile node returns to its home network, the mobile node deregisters with its home agent.

These registration processes involve the exchange of registration requests and registration reply messages. When registering using a foreign agent, the registration process takes the following steps, which the subsequent illustration depicts:

1. The mobile node sends a registration request to the prospective foreign agent to begin the registration process.
2. The foreign agent processes the registration request and then relays it to the home agent.
3. The home agent sends a registration reply to the foreign agent to grant or deny the request.
4. The foreign agent processes the registration reply and then relays it to the mobile node to inform it of the disposition of its request.

**Figure 1–7 Mobile IP Registration Process**



When the mobile node registers directly with its home agent, the registration process requires only the following steps:

1. The mobile node sends a deregistration request to the home agent.
2. The home agent sends a registration reply to the mobile node, granting or denying the request.

Also, a reverse tunnel might be required by either the foreign agent or the home agent. If the foreign agent supports reverse tunneling, the mobile node uses the registration process to request a reverse tunnel. The mobile node does this by setting the reverse tunnel flag on in the mobile node's registration request.

**Network Access Identifier (NAI)**

AAA servers, in use within the Internet, provide authentication and authorization services for dial-up computers. These services are likely to be equally valuable for mobile nodes using Mobile IP when the nodes are attempting to connect to foreign domains with AAA servers. AAA servers identify clients by using the Network Access Identifier (NAI). A mobile node can identify itself by including the NAI in the Mobile IP registration request.

Since the NAI is typically used to identify the mobile node uniquely, the mobile node's home address is not always necessary to provide that function. Thus, it is possible for a mobile node to authenticate itself, and be authorized for connection to the foreign domain, without even having a home address. To request that a home address be assigned, a message containing the mobile node NAI extension can set the home address field to zero in the registration request.

**Mobile IP Message Authentication**

Each mobile node, foreign agent, and home agent supports a mobility security association between the various Mobile IP components, indexed by their security parameter index (SPI) and IP address. In the case of the mobile node, this address is its home address. Registration messagesbetween a mobile node and its home agent are authenticated with the Mobile-home authentication extension. In addition to Mobile-home authentication, which is mandatory, you can use the optional Mobile-foreign agent and Home-foreign agent authentications.

**Mobile Node Registration Request**

A mobile node registers with its home agent using a **registration request** message so that its home agent can create or modify a mobility binding for that mobile node (for example, with a new lifetime). The foreign agent can relay the registration request to the home agent. However, if the mobile node is registering a co-located care-of address, then the mobile node can send the registration request directly to the home agent.

**Registration Reply Message**

A mobility agent returns a **registration reply** message to a mobile node that has sent a registration request message. If the mobile node is requesting service from a foreign agent, that foreign agent receives the reply from the home agent and subsequently relays it to the mobile node. The reply message contains the necessary codes to inform the mobile node about the status of its request, along with the lifetime granted by the home agent, which can be smaller than the original request. The registration reply can also contain a dynamic home address assignment.

**Foreign Agent Considerations**

The foreign agent plays a mostly passive role in Mobile IP registration. A foreign agent adds all registered mobile nodes to its visitor table. It relays registration requests between mobile nodes and home agents, and, when it provides the care-of address, de-encapsulates datagrams for delivery to the mobile node. It also sends periodic agent advertisement messages to advertise its presence.

If reverse tunnels are supported, the foreign agent establishes appropriate routes to reverse tunnel all the data packets from the mobile node for a correspondent node. A foreign agent that supports reverse tunnels advertises that the reverse tunnel is supported for registration. Given the local policy, the foreign agent can deny a registration request when the reverse tunnel flag is not set. Also, the foreign agent can only distinguish two different mobile nodes with the same IP address when the mobile nodes visit on two different advertising interfaces.

**Home Agent Considerations**

Home agents play an active role in the registration process. The home agent receives registration requests from the mobile node (perhaps relayed by a foreign agent), updates its record of the mobility bindings for this mobile node, and issues a suitable registration reply in response to each. The home agent also forwards packets to the mobile node when the mobile node is away from its home network.

A home agent might not have to have a physical subnet configured for mobile nodes. However, the home agent must recognize its mobile node's home address through the mipagent.conf file or some other mechanism when the home agent grants registration.

**Dynamic Home Agent Discovery**

In some cases, the mobile node might not know its home agent address when the mobile node attempts to register. If the mobile node does not know its home agent address, the mobile node can use dynamic home agent address resolution to learn the address of its home agent. In this case, the mobile node sets the home agent field of the registration request to the subnet-directed broadcast address of the mobile node's home network. Each home agent that receives a registration request with a broadcast destination address rejects the mobile node's registration by returning a rejection registration reply. By doing so, the mobile node can use the home agent's unicast IP address indicated in the rejection reply when the mobile node next attempts registration.

**Routing Datagrams to and From Mobile Nodes**

This section describes how mobile nodes, home agents, and foreign agents cooperate to route datagrams to and from mobile nodes that are connected to a foreign network.

**Encapsulation Types**

Home agents and foreign agents support tunneling datagrams using one of the available encapsulation methods (IP in IP Encapsulation, Minimal Encapsulation, or Generic Routing Encapsulation). Mobile nodes that use a co-located care-of address can receive tunneled datagrams using any encapsulation type.

**Unicast Datagram Routing**

When registered on a foreign network, the mobile node chooses a default router using the following rules:

1. If the mobile node is registered using a foreign agent care-of address, then the mobile node chooses its default router from among the router addresses advertised in the ICMP router advertisement portion of that agent advertisement message. The mobile node can also consider the IP source address of the agent advertisement as another possible choice for the IP address of a default router.
2. If the mobile node is registered directly with its home agent using a co-located care-of address, then the mobile node chooses its default router from among those advertised in any ICMP router advertisement message that it receives. The chosen default router network prefix must match the mobile nodes externally obtained care-of address. If the mobile node's externally obtained care-of address matches the IP source address of the agent advertisement under the network prefix, the mobile node can also consider that IP source address as another possible choice for the IP address of a default router.
3. If the mobile node is registered, a foreign agent that supports reverse tunnels routes unicast datagrams from the mobile node to the home agent through the reverse tunnel.

**Broadcast Datagrams**

When a home agent receives a broadcast datagram, it does not forward the datagram to any mobile nodes in its mobility binding list. However, the home agent does forward the datagram if a mobile node has requested forwarding of broadcast datagrams. For each registered mobile node, the home agent forwards received broadcast datagrams to the mobile node; the method depends on how the configuration of the home agent specifies categories of broadcast datagrams forwarded to mobile nodes. Broadcast datagrams over reverse tunnels are not supported.

**Multicast Datagram Routing**

To receive multicasts, a mobile node joins the multicast group in one of the following ways:

1. If a multicast router exists on the visited subnet, the mobile node uses this local multicast router. If the mobile node is using a co-located care-of address, it uses this address as the source IP address of its Internet Group Management Protocol (IGMP) messages. Otherwise, it uses its home address.
2. If the mobile node's home agent is a multicast router, the mobile node can join groups using a bidirectional tunnel to its home agent. The mobile node tunnels IGMP messages to its home agent. The home agent then forwards multicast datagrams down the tunnel to the mobile node.

A mobile node that sends datagrams to a multicast group also has the following options:

1. Send directly on the visited network
2. Send through a tunnel to its home agent

Multicast routing depends on the IP source address. Therefore, a mobile node that sends multicast datagrams directly on the visited network uses a co-located care-of address as the IP source address. Similarly, a mobile node that tunnels a multicast datagram to its home agent uses its home address as the IP source address of both the multicast datagram and the encapsulating datagram. This second option assumes that the home agent is a multicast router.

In the case of reverse tunnels, multicast datagrams are not routed through reverse tunnels. The multicast datagrams are routed as previously described.

**Security Considerations**

In many cases, mobile computers use wireless links to connect to the network. Wireless links are particularly vulnerable to passive eavesdropping, active replay attacks, and other active attacks.

Though Mobile IP cannot reduce or eliminate this vulnerability, Mobile IP can authenticate the Mobile IP messages. The default algorithm used is MD5, with a key size of 128 bits. The default operational mode requires that this 128–bit key precede and succeed the data to be hashed. The foreign agent also supports authentication using MD5 and key sizes of 128 bits or greater, with manual key distribution. Mobile IP can support more authentication algorithms, algorithm modes, key distribution methods, and key sizes.

Tunneling can be a significant vulnerability, especially if registration is not authenticated. Also, the Address Resolution Protocol (ARP) is not authenticated, and can potentially be used to steal another host's traffic.

**8: Economics of Wireless Network**

**Q1: Explain the main factors of change in economics of wireless technology.**

**Ans:-**

1. Terminal Manufacturers

2]Role of Government

3]Infrastructure manufacturers

4]Mobile Carriers

[\*For more detail ref chapter no:14 from Wireless Network-P. Nicopolitidis :page no382 to 387]